ICNL Briefer

TRENDS IN DIGITAL LAWS IN ASIA AND THE PACIFIC

Introduction

Regulating digital spaces such as the internet and social media has become a top priority for many countries. According to the Civic Freedom Monitor (CFM) at the International Center for Not-for-Profit Law (ICNL), 46 countries, including 16 countries in Asia, have passed, amended, or proposed laws and regulations to digital rights, internet governance, and social media platforms in the last decade.

This briefer provides illustrative examples of existing and pending digital laws in 17 countries in Asia and the Indo-Pacific, drawing from the CFM and additional research by ICNL.[1] This briefer is not intended to be a comprehensive compilation of all digital laws in the region but rather an overview of key trends and issues.

Key subjects of regulation in the digital sphere in Asia include criminalization and censorship of online expression, surveillance, data protection, internet access and infrastructure, and artificial intelligence (AI) governance.

Criminalization and Censorship of Online Expression

More than a dozen countries have recently passed or introduced legal measures that either criminalize or censor expression online, often empowering the government to do both. These laws affect all types of content published on the internet, including on social media platforms. In some countries, governments regulate online speech through "cybersecurity" or "online safety" laws, while other countries include provisions that restrict online expression through telecommunications or information technology laws. Regardless of the categorization, these laws tend to contain two components: 1) criminalization of speech that is protected under international law, and 2) a "take-down" regime that empowers authorities to compel removal of online content by private users, sometimes setting up liability for individuals or intermediary service providers.

Within the category of laws that criminalize and censor online expression, some countries have established specific legal measures against two types of speech: "fake news" and lèse-majesté, which often give rise to additional or more severe penalties.

1 Countries examined in Asia and the Indo-Pacific include Bangladesh, Cambodia, China, India, Indonesia, Japan, Malaysia, Mongolia, Myanmar, Nepal, South Korea, Sri Lanka, Taiwan, Thailand, and Timor-Leste.

These measures are often included in broader laws regulating online speech or regulated through the criminal code.

Laws That Restrict Online Expression

Laws, policies, and regulations restricting online expression are among the most common legal measures affecting civic space that ICNL has tracked in recent years. Examples are listed below.

BANGLADESH

The Digital Security Act (DSA) of 2018, prohibited numerous broad and vague categories of speech, and criminalized "false information," insults, and defamation. The DSA gave authorities broad powers to access and control online "data information," including content posted by individual users on social media platforms and other websites. According to the Centre for Governance Studies, between October 2018 and August 2022, the DSA has been used to charge individuals in 1,029 cases, including against 280 journalists. In September 2023, the government replaced the DSA with the Cyber Security Act (CSA), which has retained the substance of the DSA, including criminal provisions of online speech and authorities' powers to control data and access information. Although the CSA has reduced criminal punishments for most criminal acts and made certain offenses bailable, there is significant concern that it will be used to suppress expression online like the DSA has. The CSA continues to grant authorities broad powers to control, access, and censor online content.

INDIA

Section 66A of the Information Technology Act ("IT Act") criminalized "sending offensive messages through communication service, etc.," including information that was "grossly offensive" (66A(a)) and electronic mail "for the purpose of causing annoyance or inconvenience" (66A(c)). Until 2015, the police used Section 66A repeatedly to arrest those who published online and social media content critical of the government and to censor online content. In 2015, Section 66A was found unconstitutional by the Supreme Court, which deemed that internet content could not be removed without a court order. However, the Court upheld the validity of Section 68B, allowing the government to block websites whose content "has the potential to create communal disturbance, social disorder, or affect India's relationship with other countries." In addition, even after its reversal, as of 2019, Section 66A reportedly has remained in use by some local police and courts.

INDONESIA

Law No. 11 of 2008 regarding Electronic Information and Transactions ("EIT Law") criminalizes internet-based insults and defamation, with stronger penalties than those regulated in the Criminal Code (up to six years of imprisonment and Rp. 1 billion, or approximately $100k USD). According to Amnesty International Indonesia,

the government has used the EIT Law to charge at least 332 individuals, mostly for defamation, between January 2019 and May 2022.

MONGOLIA

The Government proposed a draft Law on Protection of Human Rights on Social Networks in January 2023 that included vague and broad categories of prohibited speech and established government power to censor social media content and shut down internet access. The draft Law was vetoed after public outcry and a petition to the President, but lawmakers have indicated that the law will be re-drafted and resubmitted to the Parliament.

MYANMAR

The 2013 Telecommunications Law ("Telecom Law") contains numerous provisions that restrict the freedom of expression, including the prohibition of the use of a telecommunications network to "extort, coerce, defame, disturb, cause undue influence or threaten any person." The Telecom Law is used extensively to suppress political dissent. The 2004 Electronic Transactions Act and the Criminal Code were amended following the February 2021 military coup to establish criminal liability for individuals engaging in "misinformation or disinformation with the intent of causing public panic" or otherwise expressing critical statements of the regime. The junta has also introduced a draft cybersecurity law which would, if enacted, restrict online expression even further and ban the use of VPNs, among other draconian provisions.[2]

SRI LANKA

The Government proposed the Online Safety Bill on September 15, 2023. This Bill contains vague and broad provisions criminalizing "fake" speech, establishes a "takedown" regime that would allow the authorities to require removal or blocking of content by service providers, and contains broad power for the authorities to access and obtain online data information from private individuals and users with few procedural safeguards.

"Myanmar's 2004 Electronic Transactions Act and the Criminal Code were amended following the February 2021 military coup to establish criminal liability for individuals engaging in "misinformation or disinformation with the intent of causing public panic" or otherwise expressing critical statements of the regime.

2 Although the cybersecurity law remains a draft, the military is reportedly enforcing its provisions and arresting individuals for alleged violations such as using a VPN.

THAILAND

Thailand has issued several decrees which impact speech and privacy online, particularly when combined with laws like the lèse-majesté provision in Thailand's Criminal Code (see section "Lèse-Majesté" below). A new decree that entered into force in December 2022 requires service providers to comply with content-takedown requests made by the Ministry of Digital Economy and Society within 24 hours, while a March 2023 decree allows telecommunication companies to provide user data to the police and other agencies.

TIMOR LESTE

The Government proposed a draft Cybercrime law in 2021 that reintroduces criminal defamation and criminal penalties for other categories of speech and "fake news" and proposes to increase authorities' ability to access data information.

VIETNAM

In 2023, the government amended its Telecommunications Law to require social media networks to verify users' identities and disable accounts that are not verified. Experts on digital rights and press freedom have expressed concern that these measures take away the ability of speaking anonymously – a right in international law – and will make it difficult for people to express opinions that are critical of the government or its policies. Journalists, activists, and other social media users have been arrested for posting such critical content. In addition, the law creates a "takedown" system that requires social media companies to remove posts or content, including content that is critical of the government (a criminal offense under the penal code), within 24 hours.

"Fake News" Laws

In addition to those mentioned in the previous section, many countries in Asia have specific laws that criminalize "fake news" or other false information communicated online.

CAMBODIA

A July 2023 inter-ministerial *Prakas* (proclamation) was passed, granting the Ministry of Post and Telecommunications the authority to block or remove websites and social media accounts that disseminate "misleading news affecting the honor and reputation of the Royal Government." Prior to the national elections in July 2023, Cambodian authorities blocked access to several media outlets, including the Cambodia Daily Khmer, Radio Free Asia, and Kamnotra.

LAOS

In August 2023, The Ministry of Technology and Communications announced that it plans to regulate social media and prohibit any individuals within the country from using social media to share "false news, distort information, or criticize the government."

MALAYSIA

Although the Anti-Fake News Act of 2018 was repealed in 2019, the government has continued to arrest and charge individuals under "fake news" and "disinformation" provisions of Section 233 of the Communications and Multimedia Act 1998 and Section 505(b) of the Penal Code (on statements conducive to public mischief).

TAIWAN

Article 63 of the Social Maintenance Act prohibits the "spreading of rumors in a way that is sufficient to undermine the public order and peace." In 2021, four people were fined for social media posts with "inaccurate information."

THAILAND

Under the Computer Crime Act, Section 14(2) has been used to prohibit the spread of "false computer data" in a manner likely to cause damage to national security or stir up public agitation. During COVID, the government also declared a state of emergency, empowering authorities to prevent the "distortion of information" under Emergency Decree Issue 27.

VIETNAM

In addition to amendments to the Telecommunications Law discussed above, the government passed a separate decree during COVID-19 that imposed a fine of up to $8,600 USD for posting of information that is "not suitable to the interests of the country and the people" or that is "distorted, fabricated or causing confusion among people." In 2022, the government established updated rules that allowed for takedown of "false" content on social media within 24 hours, with "very sensitive information" required to be taken down within three hours.

Lèse-majesté

At least three countries in Southeast Asia prohibit speech that insults the monarch, a criminal offense known as "lèse-majesté." As more laws regulate speech online, prosecutions for lèse-majesté will likely increase and increasingly target online speech.

CAMBODIA

The Cambodian government amended its Criminal Code in 2018 to include the offense of lèse-majesté. Since 2018, authorities

Although Malaysia's Anti-Fake News Act of 2018 was repealed in 2019, the government has continued to arrest and charge individuals under "fake news" and "disinformation" provisions of Section 233 of the Communications and Multimedia Act 1998 and Section 505(b) of the Penal Code.

have charged individuals in fifteen cases with lèse-majesté, including in one instance based on video footage of a private Zoom call among three environmental activists.

MALAYSIA

The Sedition Act criminalizes insults to the royal family and has been used more broadly to restrict speech regarding religion, race and royalty. Activists and journalists have been charged under both the Sedition Act and Malaysia's Communication and Multimedia Act for online expression.

THAILAND

The Criminal Code prohibits defamation, insults and threats against the monarchy under Section 112, which mandates up to a 15-year sentence. Between 2020 and 2022, more than 200 individuals have been charged with lèse-majesté, more than a hundred of which dealt with online expression, such as sharing videos or posting on Facebook or Twitter.

Surveillance

Surveillance is another significant trend in Asia, where many governments surveil their citizens through legal and extralegal means.[3] Several countries have used cybercrime or cybersecurity laws to give the government broad powers to surveil its citizens online. Although surveillance is not prohibited under international law, procedural safeguards must exist, including the requirement of a warrant, an appropriate threshold for state action, i.e. "reasonable grounds to believe", limited duration and scope, and inclusion of process for the protection and disposal for any data collected.

CAMBODIA

The 2015 Law on Telecommunications contains provisions that give the government sweeping powers to spy on electronic communications and criminalize communications deemed to cause "national insecurity," among other reasons. The draft Cybercrime Law, first proposed in 2012 and updated in 2020 and 2022, would require service providers to "preserve traffic data" for at least 180 days and share the data with "competent authorities" upon request.

HONG KONG

The 2020 National Security Law empowers the police to search electronic devices, intercept communications, and conduct covert surveillance on anyone suspected (on reasonable grounds) of being involved in the commission of an offense endangering national security.

3 Surveillance technologies are often deployed even where there is no legal provision, such as in India's Telangana state, where technologies such as facial recognition are used at extremely high levels in public spaces and neighborhoods despite legal restrictions on taking and sharing of private individuals' photographs with the police. See https://www.amnesty.org/en/latest/news/2021/11/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/.

SRI LANKA

The 2023 draft Online Safety Bill would allow the Minister of Public Security to appoint "experts" who can require any person to disclose any traffic data or produce documents or information without a warrant.

THAILAND

The 2017 Computer Crime Act allows the government broad authority to conduct surveillance, including warrantless searches of personal data. The investigative powers under the Act permit appointed officials by the Minister of Digital Economy to request traffic data from service providers and require providers to surrender user-related data without a warrant or any court supervision or order.

Data Protection Laws

Several countries have passed data protection laws, some of which raise concerns about the right to privacy and freedom of expression. Generally speaking, data protection laws are a positive step toward protecting the right to privacy in online spaces. However, for data protection laws to be effective, they must contain certain safeguards, which many laws and draft legislation lack. For example, data protection authorities should be independently established, rather than housed under a different department of the government, such as the Ministry of Justice or Communications. This prevents the likelihood of political influence or control by the ruling government. The government should not have broad exemptions from compliance with the law. Exceptions should be clearly defined and limited and subject to transparency and oversight criteria. In addition, effective data protection laws should also contain safeguards such as data storage limitations, collection minimization, confidentiality, accountability, and accuracy.[4]

In Asia, several countries have either passed or plan to pass legislation on data protection. In most instances, the data protection law raises concerns about one or more of the issues discussed above, such as the independence of the enforcement authority and overly broad exemptions for government adherence to the law. By contrast, South Korea's recent amendments to its data protection law have strengthened data subjects' rights.

BANGLADESH

In 2023, the Government proposed two drafts of the Data Protection Act (DPA). Although the more recent August 2023 amended version includes some positive improvements such as removal of criminal penalties for violations and requirement of data storage within Bangladesh, the current draft DPA retains some problematic provisions. For

4 An example of a good data protection law is the European Union's GDPR, which enshrines eight user rights: to information, access, rectification, erasure, restriction of processing, to object, portability, and to avoid automated decision-making/right to explanation.

example, the DPA contains an overly broad scope of data control. It also provides broad exemptions for data protection for public interest that would likely allow government authorities broad exemption from abiding by data protection principles. Like the previous version of the draft Act, there is concern about the independence of the data protection board set up under the DPA.

CAMBODIA

Similar to Bangladesh, Cambodia has also proposed a Draft Law on Personal Data Protection in 2023. The Draft Law provides oversight power to the Ministry of Post and Telecommunications (as opposed to the general best practice of establishing an independent data protection office) and contains broad exemptions for obtaining consent and protecting personal data under the Law. Additionally, the Draft Law would require data localization, which might increase the ability of authorities to access private data and surveil citizens, and high fines and imprisonment for egregious violations of the Law.

CHINA

Under China's recent laws like the 2021 Personal Information Protection Law and 2021 Data Security Law, the government imposes harsh penalties for private companies' breach of security or failure to obtain user consent for data collection while largely exempting the government. In 2021, the Supreme People's Court of China found that individuals have a technical right to opt out of facial recognition. In August 2023, the cyber regulator in China released draft regulations on facial recognition technology that, while continuing to allow state surveillance, gives individuals the right to protect their personal data, i.e. intimate data of one's face, for commercial purposes.

INDIA

India passed the Digital Personal Data Protection Act on August 9, 2023, providing some limited user data protection. However, the Act raises several concerns regarding the right to privacy, for instance by giving wide powers to the State to process data without consent, including during periods that pose a threat to public health. The Act also establishes a regulatory board that is likely to be subject to political influence. It is also unclear how this Act might interact with the existing Right to Information Act.

> **Recently, South Korea amended its 2011 Personal Information Protection Act, which came into effect in September 2023. Several amendments represent positive changes that strengthen data subjects' rights, such as enshrining the right to data portability and the right to object, reject, or request explanations to automated decision-making.**

INDONESIA

The Personal Data Protection Law ("PDP Law") was passed on October 17, 2022, requiring compliance within two years. The PDP Law establishes exemptions for data protection for broad categories such as national defense and security and public interest. In addition, the data protection authority is appointed by the President and raises concerns of independence.

SOUTH KOREA

Recently, South Korea amended its 2011 Personal Information Protection Act (PIPA), which came into effect in September 2023. Several amendments represent positive changes that strengthen data subjects' rights, such as enshrining the right to data portability (data subjects' right to request personal data be transmitted to themselves or a third party that satisfies security standard in the Enforcement Decree) and the right to object, reject, or request explanations to automated decision-making. The amendments also establish data handlers' obligation to destroy pseudonymized data and substitute criminal penalties with administrative penalties for data breaches caused by failure to take data protection measures.

Internet Access and Infrastructure

Several countries in Asia have passed legislation enabling authorities to control internet and other telecommunication services, including by proposing a government-controlled national internet gateway.[5] These laws run the risk of enabling broad government control of online expression and limiting access to information.

CAMBODIA

In 2021, the Government introduced via a sub-decree a controversial National Internet Gateway (NIG) that would allow the authorities to monitor and control online traffic by routing all internet traffic, including from overseas, through a single portal managed by a government-appointed regulator. Under the decree, the operator of the gateway would support the authorities to disconnect network connections for a number of vague and broad reasons. The decree, if implemented, would require internet service providers (ISPs) to compel users to register their identities and connect networks to the gateway or face consequences such as suspension of operating licenses and freezing of bank accounts. The proposed decree was met with criticism from various stakeholders, including from social media platforms. Plans for the implementation of the NIG have been postponed.

MYANMAR

Article 77 of the Telecom Law allows the Ministry of Communications and Information Technology to suspend telecom services in emergency situations, which has been

5 An internet gateway is a central point that all internet data must pass through. A national gateway such as the one proposed in Cambodia creates a centralized gateway, controlled by the government, that regulates the flow of internet data to and from all other networks.

used to justify extensive internet blackouts. Because the law establishes no criteria for triggering internet suspension, the government has used the provision to arbitrarily shut down internet and mobile communications, often before crackdowns on peaceful demonstrations.

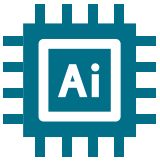
NEPAL

In August 2023, the government approved a new National Cyber Security Policy, which introduced concerning proposals regarding a government-owned intranet and a national internet gateway, the details of which have not yet been communicated by the government. There is concern that the national gateway would enable the government to control all internet traffic in the country through a government-appointed operator, expanding abilities to surveil and censor internet users and violate rights to privacy.

THAILAND

In 2015, the Government proposed the establishment of a national internet gateway that would establish a firewall to filter all internet traffic in and out of Thailand. This proposal faced significant backlash and criticism and was eventually tabled. In 2022, the Digital Economy and Society Minister announced plans to resurrect a proposed national internet gateway. In the proposal, the Minister cited Cambodia's NIG proposal as an impetus for reviving the plan.

AI Governance



With the increase in use of AI across the globe, more countries are responding by proposing AI governance measures at the national level. Although no country has passed binding legislation in Asia and the Pacific on AI ethics and governance, several countries have adopted or plan to adopt principles or strategies.

INDONESIA

The Ministry of Communication and Information plans to release a Circular Letter at the end of 2023 on AI governance, incorporating Indonesia's National AI strategy and the UNESCO principles in its Ethical AI Recommendation. It is unclear whether AI ethics legislation would follow the Circular Letter, which would not be legally enforceable.

JAPAN

Japan adopted the Social Principles of Human-Centric AI in 2019. The Principles set forth human dignity, diversity and inclusion, and sustainability as core philosophies, with the objective of protecting and realizing these principles through AI. The Principles correspond to OECD's AI Principles.

SRI LANKA

The government has plans to prepare and publish an AI national strategy in 2024.

Conclusion

Governments in Asia and the Indo-Pacific are seeking to regulate the expanding universe of online activity, social media, and rise in digital technologies. In many instances, governments have passed laws and regulations that restrict or erode the rights of freedom of expression, assembly, and association, as well as the right to privacy.

Digital laws that restrict and criminalize expression online, hinder access to information, and give the government latitude to access individuals' private information have a significant impact on fundamental civic freedoms. As countries across the region are experiencing rollbacks in democratic governance and respect for human rights, the digital space has become an increasingly important forum for accountability, transparency, and social justice. As information becomes more expeditiously disseminated online and through social media platforms, the survival of a robust civic space depends on the protection of digital rights and freedoms.

At the same time, in digital policymaking, civil society plays a critical role in ensuring that governments strike the right balance and regulate in ways that protect and promote international human rights laws and standards and enable a vibrant civic space. In several countries mentioned in this briefer, such as Mongolia, Bangladesh, Cambodia, and Thailand, civil society coalitions were crucial in preventing the passage of restrictive and repressive laws or successfully calling for legal reform of existing restrictive legislation. As governments respond to needs for regulation on emerging issues like personal data protection and AI governance, engagement with civil society is essential to ensure that new laws regulating digital technologies protect human rights and civic freedoms.