ICNL

www.icnl.org
info@icnl.org

Summary Analysis

Cambodia's Draft Law on Digital Government of the Kingdom of Cambodia

Introduction

In June 2025, Cambodia's Ministry of Post and Telecommunications (MPTC) circulated a draft Law on Digital Government of the Kingdom of Cambodia (Law). The Law aims to set forth the principles and mechanisms to build digital governance in Cambodia through information and communication technologies.

At the request of partners, the International Center for Not-for-Profit Law (ICNL) prepared this summary analysis to provide civil society organizations, the Government of Cambodia and other stakeholders with an overview of international human rights law and global norms and principles on digital governance.

This summary analyzes the English version of the Law shared by the MPTC when requesting inputs from civil society and development partners. Rather than addressing every aspect of the Law, ICNL's analysis summarizes key issues and best practices in digital governance to aid in revising the draft law.

International Law

Cambodia ratified the International Covenant on Civil and Political Rights (ICCPR) in 1992. The right to freedom of expression is guaranteed by Article 19 and the right to privacy is guaranteed by Article 17 of the ICCPR.

Right to Freedom of Expression: Article 19 protects the right to freedom of expression, which encompasses the right to hold opinions without interference, and the freedom to seek, receive, and impart information and ideas of all kinds through any medium regardless of frontiers.[1]

States are obligated to guarantee the right to freedom of expression. The Human Rights Committee has stated that "any restrictions on the operation of websites, blogs, or any other internet-based electronic or other such information dissemination systems" must comply with Article 19.[2]

[1] Cambodia signed the ICCPR in 1992.
[2] Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of opinion and expression*, UN Doc. CCPR/C/GC/34 (2011), para. 43.

Restrictions on the speech and expressions guaranteed in Article 19 are lawful only when such restrictions pass a three-part, cumulative test derived from Article 19, as follows:

> (1) **Principle of legality:** the restriction must be clearly articulated in the law such that a person reading the law can easily understand how to comply with the law and the consequences of violating the law;
>
> (2) **Principle of legitimacy**: the restriction must pursue one of the purposes set out in Article 19(3) of the ICCPR, namely: (i) to protect the rights or reputations of others; or (ii) to protect national security or public order, or public health or morals; and
>
> (3) **Principle of proportionality**: the restriction must be proven as the least restrictive means required to achieve the purported aim.[3]

Right to Privacy: Article 17 of the ICCPR bars arbitrary or unlawful interference with "privacy, family, home, or correspondence." Restrictions on privacy must meet the legality, legitimacy, and necessity standards,[4] meaning that the government's ability to interfere with an individual's privacy rights must be clearly written into law, for a valid purpose, and both proportional in scope and directly related to that purpose. Government surveillance that is broad, indefinite, or secretive is a violation of international law.

In General Comment 16, the Human Rights Committee stipulated that the ICCPR not only prevents States from violating the right to privacy in ways inconsistent with Article 17, but also requires States to institute a legal framework to prohibit violations of privacy by private individuals and entities.[5] Such law must give individuals the right to know "what personal data is stored in automatic data files, and for what purposes," and "which public authorities or private individuals or bodies control or may control their files." They should also have the right to request correction of incorrect data and elimination of the data altogether. This framework forms the basis of the rights that are included in modern data protection laws, such as the European Union's General Data Protection Regulation (GDRP): the right to be informed, right of access, the right to rectification, and the right to erasure (also referred to as the right to be forgotten).[6]

The right to privacy is closely linked to Article 19's right to freedom of opinion and expression because individuals who know or fear that their communications are being monitored by the government are less likely to express themselves freely for fear of reprisal. Similarly, when information that an individual privately communicates online is used against them in judicial

---

[3] See, e.g., United Nations Human Rights Council, *Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, U.N. Doc. A/HRC/17/27 (2011), para. 69.

[4] Electronic Freedom Foundation and Article 19, "Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance," (May 2014), https://www.article19.org/data/files/medialibrary/37564/N&P-analysis-2-final.pdf.

[5] "States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons. . .. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law." UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy)* (1988) para. 10.

[6] It should be noted that the GDPR includes additional rights, such as the right to data portability (the ability to obtain personal data in a format that can be used in other contexts), the right to restrict or object to the processing of personal data, and the right not to be subject to a decision based solely on automated processing of personal data. Data Protection Commission, *Your Rights Under the GDPR*, https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation.

proceedings or extra-judicial recrimination, the effect is to curtail speech and deter others from freely communicating their thoughts and opinions through online sites and applications.[7] Thus, a state's failure to adequately protect the right to privacy, whether online or offline, can also pose grave risks to an individual's right to freedom of expression.

Good digital governance starts from recognizing and ensuring that the human rights that individuals enjoy offline be protected online, including the right to freedom of opinion and expression, the right not to be subject to arbitrary or unlawful interference with privacy, and other human rights and fundamental freedoms.

Key concerns

LACK OF SPECIFICS

The Law outlines several initiatives to create a robust digital governance infrastructure. However, the details of many of these initiatives are left open. The Law simply says that these processes, safeguards, guidelines, etc. will be determined by a Sub-Decree. Examples include: Guidelines on Management and Use of Data Center and Government Cloud; [8] the organization, management, and use of digital ID infrastructure and Verified Digital ID Account; [9] the establishment and management of a national data repository; [10] the preparation, management, and use of bulky data exchange platform; [11] the preparation, management, and use of national payment gate infrastructures; [12] the preparation, management, and use of government common systems; [13] standards, specifications and accessibility of Government digital services; [14] the Digital Government Interoperability Framework;[15] the digital payment gateway infrastructure;[16] guidelines on Data Governance;[17] guidelines on accessing government held data;[18] and management and use of data at the sub-national level,[19] amongst others.

These examples make up nearly all of the new digital governance infrastructure and all are likely to affect the exercise of human rights. The Law should include the details of how these systems will operate. By leaving this to future sub-decrees it is impossible for the Cambodian people to know how digital governance will affect their lives, their ability to access government services and their ability to exercise fundamental human rights. Furthermore, since sub-decrees are drafted and enacted via internal mechanisms of ministries, it removes public participation from the law-making process. Rather than build off of the current approach by the MPTC to hold consultations with non-governmental stakeholders and make

[7] U.N. Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," A/HRC/23/40 (April 2013), para. 30, 47-49.
[8] Law, Article 10.
[9] Law, Article 11.
[10] Law, Article 12.
[11] Law, Article 13.
[12] Law, Article 14.
[13] Law, Article 16.
[14] Law, Article 17.
[15] Law, Article 18.
[16] Law, Article 19.
[17] Law, Article 25.
[18] Law, Article 29.
[19] Law, Article 30.

the draft of the Law available to the public, the sub-decree process will remove this collaboration.

Article 25(a) of the International Covenant on Civil and Political Rights recognizes the right to take part in the conduct of public affairs. In 2018, the UN Human Rights Council created the UN Guidelines on the Right to Participate in Public Affairs to explain how governments should effectively and meaningfully provide for this right during the policymaking process. The Guidelines outline several recommendations, including that governments must provide "sufficient time for rights holders to prepare and make their contributions during decision-making processes." All stakeholder groups, particularly those most impacted by the legislation, should have different means to contribute feedback, including in writing and during in-person gatherings. Moreover, the opportunities for consultation should begin when the government initially announces a proposal to enact a new legislation or policy, the drafting process should be transparent, and there should be multiple opportunities to provide feedback. According to the UN Guidelines, consultations also have the benefit of increasing the legitimacy and trust in government institutions.

Therefore, ICNL recommends that the Law include the specifics of how these new processes and infrastructure will operate, including detailed guidelines to ensure transparency and accountability, inclusivity and non-discrimination, and privacy and security. ICNL also recommends additional, longer periods of consultations with privacy, cybersecurity, and human rights experts and more opportunities for the public to understand the proposed legislation and provide input.

LACK OF INDEPENDENCE AND OUTSIDE EXPERTISE

The Law calls for the establishment of a Digital Government Committee, which is essentially the body charged with executing the building and management of Cambodia's digital governance and implementing the Law.[20] This committee will be led by the Minister of the MPTC and composed of members from other ministries and government institutions. The details of the Committee's members, organization and functioning will be determined by a sub-decree.

The Digital Government Committee lacks independence and expertise from non-governmental stakeholders. Independence is regarded as essential to creating rights-respecting digital governance infrastructure and processes.[21] Including experts in the Digital Government Committee from academia, civil society and/or the business community would create a more transparent, accountable body that is better equipped to efficiently and effectively deal with issues that arise during the transformation to e-governance.

---

[20] Law, Article 4: Digital Government Committee. The Digital Government Committee shall be established with the purpose of ensuring the efficiency and effectiveness of performing the roles as executing body for the National Digital
Economic and Social Council on technical work and policies in leading, facilitating, and promoting the building of digital government of the Kingdom of Cambodia. The Digital Government Committee shall be led by the Minister of the Ministry of Post and Telecommunications and be composed of members from relevant ministries and institutions. The Digital Government Committee shall have a General Secretariat as executing body. The organization and functioning of the Digital Government Committee shall be determined by Sub-Decree.

[21] See, e.g., The Universal Digital Public Infrastructure - A Guide to Building Safe and Inclusive DPI for Societies, Annex 4, noting that independent institutions are a requirement and key indicator to ensure to ensure and assure safety and inclusion of people.

Without independence, there is considerable risk that the Digital Government Committee could be politically weaponized and used to target CSOs, human rights defenders, media outlets, political parties, or other entities that might criticize the implementation of digital governance infrastructure. Creating an independent Digital Government Committee with diverse stakeholders would mitigate the risks of political considerations influencing the Committee's decisions while including real world expertise that would ultimately help create an effective transition to e-governance.

UNCLEAR REQUIREMENTS FOR DIGITAL PAYMENTS

The Law establishes a Digital ID infrastructure to facilitate digital payments.[22] This infrastructure will enable persons and legal entities to request and pay for "public services, social security services, national postal services, water services, electricity services, and other services as decided by the Royal Government." While creating an infrastructure to facilitate digital payments for government services, with appropriate safeguards to prevent fraud, is commendable, the lack of specifics could prevent large groups of individuals from accessing government services.

First, while the requirements to create a Verified Digital ID Account that can the used for online transactions are minimal, there are several categories of people that may be unable to create such an account. These include displaced peoples who do not have a passport and economically disadvantaged individuals who do not have an identity card or driver's license, birth certificate or other required form of identification. Care should be taken to provide these individuals with a way to create a Verified Digital ID account.

Second, it is unclear if creating a Verified Digital ID is mandatory. Article 11 says that people and legal entities "may" create a Verified Digital ID account to be used for online transactions. The "may" signifies that this is choice. However, Article 19 states that "all taxes, public service fees, water fees, electricity fees, waste fees, fines and other service fees shall be paid through digital payment…"[23] Article 19 indicates that people living in Cambodia and Cambodian legal entities will only be able to pay for government services via the digital payment system, which is presumably only possible if a Verified Digital ID account is created.

Article 14 requires the development of a "comprehensive and interoperable national payment gateway" system.[24] While this is a positive development (presuming the forthcoming sub-decree that will govern the use of the system is rights-respecting), it is unclear whether a Verified Digital ID will be required to use this national payment gateway. If a Verified Digital ID is required, then the Law is essentially making it a mandatory requirement for each person and legal entity in Cambodia to obtain a Verified Digital ID, because without it they will not be

[22] Law, Article 11.
[23] Law, Article 19: Payment through digital system: All taxes, public service fees, water fees, electricity fees, waste fees, fines and other service fees shall be paid through digital payment determined by the Royal Government. The Digital Government Committee shall develop digital payment gateway infrastructure to facilitate payment through digital system. The development and management of digital payment gateway infrastructure shall be determined by Sub-Decree.
[24] Law, Article 14: Payment gateway infrastructures: The Digital Government Committee shall prepare a master plan for the development of the comprehensive and interoperable national payment gateway infrastructures, which have wide coverage on the digital payment in every sector and aspect to ensure reliable and trusted interoperability as well as the high efficiency and security of the system. The preparation, management, and use of national payment gate infrastructures shall be determined by Sub-Decree.

able to receive or pay for basic government services or make digital payments, a vital facet of Cambodia's economy. In 2023, digital payments amounted to $492 billion, which is equivalent to 16 times of Cambodia's gross domestic product.[25]

The process for making digital payments should be made clear. Avenues for people who do not have traditional forms of identification should be included so that they can receive the benefits of making digital payments. Finally, Ministries and other government institutions should continue to enable and allow for non-digital payments, especially for necessary goods and services, like water and electricity.

DATA GOVERNANCE SECURITY

Chapter 6, articles 25 through 30, discusses how the Cambodian government will store, modify, disseminate, use and share data it holds and owns. Much of this data will likely be sensitive personal data of Cambodian citizens and people living in Cambodia. However, this Chapter does not specify how the Cambodian Government will safeguard data.

The only reference to the security of data is in Article 28, which when discussing data sharing says that, "sharing of the data is [to be] done in a secured manner without causing data privacy violations or leaving data open to being hacked."[26] Even when discussing Application Programming Interfaces (APIs) to ensure electronic system integration, there is a mere passing reference to "promot[ing] safe and reliable sharing of data," but there is no requirement that APIs used by ministries contain the ability to encrypt data or use other best cybersecurity practices. As noted earlier, the guidelines for the applications and processes that will control data sharing will be developed in subsequent sub-decrees. Presumably these sub-decrees will contain requirements to keep data safe and secure, but it is troubling that these safeguards are not contained in the Law.

The Law should be revised to contain appropriate safeguards for government held data. It needs to contain specific regulatory and technical principles that enforce core privacy principles. "Personal data should be processed or retained lawfully and transparently only by authorized personnel within a legal framework including transaction history, data subject rights and protections against overreaching requests."[27] "Legal frameworks should consist of laws, policies, regulations, and codes of practice, and should establish independent oversight mechanisms, and include accessible grievance and redressal mechanisms to address violations of requirements and protected rights."[28] Storing and controlling sensitive personal data creates a huge risk to the right to privacy. To address this risk, the Law needs to contain specific safeguards to keep data safe and secure.

---

[25] See, Kiripost, *Cambodia Charts 1.8b Digital Payments, Valued at $492b in 2023*, citing statistics from the National Bank of Cambodia.

[26] Law, Article 28: Data Sharing: Ministries and institutions shall comply with the standards and specifications for data
sharing. When sharing data, ministries and institutions shall take necessary precautions to ensure that the sharing of the data is done in a secured manner without causing data privacy violations or leaving data open to being hacked. Guidelines on Data Sharing shall be determined by Sub-Decree.

[27] The Universal Digital Public Infrastructure - A Guide to Building Safe and Inclusive DPI for Societies, page 24.

[28] Nikhil Dutta and Shabnam Mojtahedi, "Navigating the Risks and Rewards of Digital ID Systems," Open Government Partnership.

Other Issues

MINISTRY SOCIAL MEDIA ACCOUNTS & FAKE NEWS: Article 22 makes it illegal to "create fake social media account of ministries and institutions and publish fake news."[29] While it is good policy to have official social media accounts for ministries, Article 22 is problematic for two reasons. First, the reference to fake news is troublesome because there is no standard definition of "fake news." It is an amorphous concept that has been used to stifle dissent and criticism of government actors and policies, which are protected speech under the ICCPR. This reference should be removed. Second, care should be taken to ensure that parody accounts or accounts that relay or repost information from ministries are exempted from this prohibition. Providing exemptions would likely be necessary to ensure compliance with Article 19 of the ICCPR.

CRITICAL DIGITAL INFRASTRUCTURE: Article 8 designates certain digital infrastructure to be "critical digital infrastructure," but, under Article 8(g), also enables the government to designate any other digital infrastructure as "critical digital infrastructure" whenever it wants for whatever reason it wants.[30] The Law lists several pieces of government operated digital infrastructure as "critical digital infrastructure," but notably does not limit "critical digital infrastructure" to these six enumerated categories and enables the Government to designate any other digital infrastructure as "critical digital infrastructure."

Critical digital infrastructure seems to be a subset of "critical information infrastructure (CII), which is the internationally recognized term." Typically, when States define something as "critical information infrastructure," it requires the owners or operators of CII to undertake additional security measures which are often overseen by government authorities. These authorities can usually access CII and in the event of emergencies take them over, shut them down or undertake other law enforcement actions.

Notably, the Law does not provide any information as to what requirements, if any, operators or developers of "critical digital infrastructure" must undertake and it does not contain prohibitions or penalties, if any, for individuals that interfere with the operations of "critical digital infrastructure."

While states have a legitimate interest in mitigating cybersecurity threats and incidents, the unfettered ability to designate any digital platform or technology as "digital information infrastructure" is problematic because it could subject civil society stakeholders to burdensome administrative procedures or state requests for access to organizational

[29] Law, Article 22: Social Media Account of Ministries and Institutions: The Ministry of Post and Telecommunications shall manage the list of social media accounts of ministries and institutions. Ministries and institutions shall notify the Ministry of Post and Telecommunications about their social media accounts. Content published on the official social media account of the ministries/institutions shall be considered as official information of the government and shall be backed up in the National Data Repository.
Persons that create fake social media account of ministries and institutions and publish fake news shall be penalized in accordance with Article 40 of this law. Guidelines on the use of social media account of ministries and institutions shall be determined by Sub-Decree.

[30] Law, Article 8: Article 8 . Critical digital infrastructures: The critical digital infrastructures designated by this law include but not limited to: a) Government private network. b) Data center and government cloud infrastructure. c) Digital ID infrastructure. d) National data repository. e) Bulky data exchange platform. f) Payment gateway infrastructure. g) Other critical digital infrastructure designated by the Royal Government.

information without enhancing the state's cybersecurity. Indeed, this risk has been identified when reviewing Cambodia's draft Cybersecurity Law.

Removing Article 8(g) will also help the MPTC apply the law in a clear and consistent manner. To address concerns that new, unforeseen technologies or platforms will need to be designated as critical digital infrastructure in the future, the Law could include a requirement to conduct and publish a risk assessment to identify critical digital infrastructure.[31]

Conclusion

ICNL appreciates the opportunity to analyze the Law. The Law does an admirable job of outlining the infrastructures needed to create digital governance in Cambodia. However, the Law is missing many of the specific details for each piece of infrastructure. Without these details, it is difficult to ensure that human rights and international best practices for digital governance will be met and protected. The Law, as currently drafted, is good starting point to create the processes and platforms for digital governance, but it needs revisions in the areas highlighted to better protect the rights of all people in Cambodia. For further information or queries, please contact ICNL's Digital Rights Team (digital@icnl.org).

[31] This is the approach adopted by the European Union when considering what infrastructure to designate as critical information infrastructure; the EU requires members to conduct national risk assessments to identify and alert specific critical entities to their "critical entity" designation; see, European Union, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM(2020)829, Article 4-5.