**LEGAL ANALYSIS: CAMBODIA DRAFT LAW ON CYBERSECURITY**[1]

In November 2022, Cambodia's Ministry of Post and Telecommunications (MPTC) announced that it had drafted a comprehensive law on cybersecurity.[2] Since then, the Ministry has been reviewing and revising the Draft Law on Cybersecurity ("Draft Law"), based on input and comments it has received from stakeholders.[3]

The aim of the Draft Law is, according to article 1, to "determine principles, rules and mechanisms to manage and maintain cybersecurity of Critical Information Infrastructures (CIIs) for the purpose of safely and sustainably ensuring essential national services". The Draft Law is made up of forty-eight provisions that are divided into ten chapters, on: general provisions (chapter 1); competent institutions (chapter 2); general principles of ensuring cybersecurity (chapter 3); managing and maintaining cybersecurity (chapter 4); licensing for cybersecurity service providers (chapter 5); cybersecurity inspection (chapter 6); dispute resolution (chapter 7); penalty provisions (chapter 8); inter-provisions (chapter 9); and final provisions (chapter 10).

Access Now and the International Commission of Jurists (ICJ) consider that the Draft Law, if adopted in its current formulation, has the potential to arbitrarily interfere with the enjoyment of the rights to privacy and freedom of expression and information, without sufficient independent oversight. Our organizations recognize the legitimacy and importance of Cambodia's objective in acting to strengthen its cybersecurity landscape to deal with malicious cyber activities. However, it is critical that any law, policy, or practice directed to that end be guided by and conform with Cambodia's international human rights obligations. In particular, we are concerned that as presently conceived, the provisions of the Draft Law contain vague and overbroad terms; would confer overbroad powers to the Digital Security Committee (DSC) and Cybersecurity Inspectors; would impose disproportionately harsh criminal sanctions; and fail to adequately guarantee the right of appeal or independent, effective mechanisms for oversight or remedy in case of abuse.

Our organizations submit that the approach of this draft law undermines its main purpose, namely to advance a framework that enables, rather than hampers, cybersecurity. The proposed draft provisions around compelling the licensing of nearly all cybersecurity services is an excessive provision that would serve to limit the ability of all residents in Cambodia from being able to secure themselves against intrusion into their networks and safeguard their data. Such threats engender particularly consequential impacts on persons from vulnerable communities as well as at-risk actors, such as journalists and human rights defenders.

**Cambodia's International Human Rights Obligations**

---

[1] This analysis is based on the Draft Law on Cybersecurity, dated 2 September 2022.

[2] Kang Sothear, "MPTC finalises more draft laws, policies on cybersecurity, posts", Khmer Times, 7 November 2022, available at: https://www.khmertimeskh.com/501180686/mptc-finalises-more-draft-laws-policies-on-cybersecurity-posts/.

[3] Based on information received by Access Now and the ICJ, the draft is still undergoing review and revisions. On 10 March 2023, it was reported that the MPTC spokesperson said, "the law is still in draft, and the team is working hard to review the comments from all stakeholders"; Fiona Kelliher, "Leaked law proposal would give Cambodia expanded powers to censor critics", Rest of World, 10 March 2023, available at: https://restofworld.org/2023/cybersecurity-law-draft-cambodia-elections/. See also, Ly Lya, "Telecommunication ministry completes draft cyber security law", The Phnom Penh Post, 11 November 2022, available at: https://www.phnompenhpost.com/national/telecommunication-ministry-completes-draft-cyber-security-law.

As a State party to the International Covenant on Civil and Political Rights (ICCPR), Cambodia is legally obligated to respect and ensure the rights to privacy and freedom of expression and information, as guaranteed by articles 17 and 19 of the ICCPR respectively. The rights to privacy and freedom of expression and information are interlinked. Effective data protection and encryption are necessary conditions to allow individuals to exercise freedom of expression online without arbitrary interference.[4] To ensure the effective enjoyment of the right to freedom of expression and information, article 19(3) expressly provides that any limitation to that right is strictly subjected to the principles of legality, i.e. it must be "provided by law." A restriction may only be made for one of the legitimate purposes specified in article 19(3), namely, to protect the rights and reputation of others, national security, public order or public health or morals. Any restriction is subject to the principles of necessity and proportionality, meaning the measures limiting rights must be necessary and the least restrictive means to achieve the legitimate purpose.[5] Finally any limitation must not be applied on a discriminatory basis or for a discriminatory purpose. These principles apply to the right to privacy in the same manner as they do to the right to freedom of expression and other fundamental freedoms, as affirmed by the UN Human Rights Committee, the UN Human Rights Council and UN Office of the High Commissioner of Human Rights.[6]

The Draft Law does not include any explicit mention to international human rights law and standards. Article 6 of the Draft Law, providing a list of the general principles that shall be upheld when ensuring cybersecurity, omits the international human rights law principles of legitimacy, legality, necessity and proportionality. The lack of a human rights-based approach to the Draft Law underpins other problematic aspects that would threaten the rights to privacy and freedom of expression and opinion.

**Effective Cybersecurity Requires a Human-Centric and Human Rights Respecting Approach**

The draft law avowedly seeks to advance the objective of strengthening cybersecurity, particularly with regards to critical information infrastructure. However, in its overall approach as well as several specific provisions (further detailed below), it would in practice likely have the opposite effect, namely making the cybersecurity situation of individuals and communities in Cambodia more perilous and at risk to cyber intrusion.

It is crucial to recognize that cybersecurity requires not only an application of the principles of legitimate purpose, necessity, proportionality and non-discrimination to any rights limitation, but also includes a positive obligation of States to take effective measures to safeguard the exercise of human rights online and offline. These should be aimed at securing the availability, confidentiality, and integrity of information and its underlying infrastructure so as to protect and enhance the security of persons both online and offline.[7]

---

[4] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, UN Doc. A/HRC/29/32, 22 May 2015 ("A/HRC/29/32"), paras. 16 – 18.

[5] See: Human Rights Committee, *General comment no. 34, Article 19, Freedoms of opinion and expression*, UN Doc. CCPR/C/GC/34, 12 September 2011 ("CCPR/C/GC/34"), paras. 21 – 36.

[6] UN General Assembly, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/39/29, 3 August 2018, para. 10; Human Rights Council, *The right to privacy in the digital age*, UN Doc. A/HRC/RES/34/7, 7 April 2017, para. 2.

[7] See, for example the definition of cybersecurity arrived after consultation and study by the Freedom Online Coalition's Working Group 1 on 'An Internet Free and Secure' in December 2014, which adopted the following working definition of cybersecurity: "PREAMBLE: International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights. DEFINITION: Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline" Freedom Online Coalition, WG 1 – An Internet Free and Secure, September 2015. Available at https://freedomonlinecoalition.com/blog/wg-1-an-internet-free-and-secure/.

The United Nation's Special Rapporteur on Freedom of Expression noted in the 2015 report on *encryption, anonymity, and the human rights framework* that restrictions on digital security tools - including encryption and anonymity more generally - may impermissibly interfere with the ability of individuals to hold opinions. To bring States into compliance with human rights obligations, the Special Rapporteur recommends that national laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online

In that context, it is clear that the draft law's proposal to require the licensing of all cybersecurity related services without any categorisation or threshold would be a grave, disproportionate measure impacting the provision of digital security in a manner undermining human rights relating to opinion, expression, and privacy. A proscription that no person can provide cybersecurity services without a licence from MPTC would render any digital security measure made accessible in Cambodia illegal unless specifically authorized by the government (article 23).

Such a proscription would likely be extremely damaging to the provision of cybersecurity itself, since the wide range of services and technologies that different individuals and organizations in Cambodia generally use to secure themselves from cyber threats and intrusion would be likely rendered inaccessible explicitly or by the chilling effect of threat of criminal liability. It would also correspondingly pose an impermissible interference on the enjoyment of human rights, by restricting access and use of all digital security tools, which constitute technologies crucial for the exercising of the rights to opinion, expression, and privacy among other protected international human rights. Additionally, it would appear this general licensing mandate is not relevant to stated purpose of the draft law, namely to advance the cybersecurity of critical information infrastructure. A general, overarching requirement for all cybersecurity services to be licensed would not impact only the provision of cybersecurity services for critical information infrastructure - it would also apply to all, non-critical digital services, transactions, and communications conducted by individuals and organizations located in Cambodia.

**Overbroad Powers of the Digital Security Committee and Cybersecurity Inspectors**

*Digital Security Committee*

The Draft Law, if adopted, would grant wide-ranging powers to the DSC that may be used to arbitrarily interfere with the right to privacy and unduly restrict the right to freedom of expression and information. The DSC is an executive body, led and coordinated by the MPTC, with the aim to "ensure efficiency and effectiveness in fulfilling the role of leading, coordinating, and promoting the governance of digital security" (article 4).

Powers granted to the DSC include, among others, the authority to order a private organization to: "provide information and allow the use of related electronic devices" with the private organization's consent, in order to prevent and mitigate risks caused by a cybersecurity threat or incident (article 19); "allow officers in charge of the DSC to access any relevant computer or computer system" where the private organization is unable to prevent and mitigate a cybersecurity incident that has reached a "critical level" (article 21); and "access computer data or other data" pursuant to a court order, in situations where a private organization is unable to terminate or mitigate the impacts caused by a cybersecurity threat (article 22).

These powers conferred on the DSC are overbroad and do not comply with the principles of legality and proportionality. Articles 19 and 21 of the Draft Law does not require the DSC to obtain prior approval from an independent and impartial judicial authority or equivalent independent and duly-mandated oversight body before issuing orders to "provide information and allow the use of related electronic devices" or allow access to "any relevant computer or

computer system". This runs contrary to the legality principle, which, in addition to requiring that provisions are stated with precision, also requires proper legal process, including that any measure that may interfere with the rights to privacy and freedom of expression and information be applied with strong judicial safeguards.[8]

Further, article 21(1) of the Draft Law, authorizing the DSC access to "any relevant computer or computer system", has the potential to unnecessarily and disproportionately interfere with the right to privacy as it is not targeted towards data that is specifically necessary to prevent a "cybersecurity threat" and may not be the least intrusive measure available towards that strictly limited aim.[9] This broad formulation may allow the DSC to access private data held on a computer system well beyond what is required by the exigencies of a situation.[10] This concern of overbroad access to private data is compounded by the absence within the Draft Law of an independent, effective oversight or remedial mechanism to safeguard against executive overreach of the DSC.

*Cybersecurity Inspectors*

The Draft Law also provides overbroad powers to Cybersecurity Inspectors, risking arbitrary interference with the rights to privacy and freedom of expression and information. Under article 24 of the Draft Law, Cybersecurity Inspectors are appointed as "judicial police officers" by the Minister of the MPTC to "monitor, study, inspect, and strengthen the enforcement of this law". Powers granted to Cybersecurity Inspectors include the powers to "investigate, observe, monitor, prevent and respond to cybersecurity threats and […] incidents" (article 26) and "check, confiscate evidence, call on involved persons, and perform other procedures in accordance with regulations of the Code of Criminal Procedure" (article 27).

At the outset, we submit that the stated objective of seeking to "monitor, prevent and respond to cybersecurity threads and […] incidents" would not be optimally realized through the operation of a newly created unit of Cybersecurity Inspectors. Cybersecurity incident response does not require an approach solely or even primarily anchored in policing and law enforcement. Indeed, strategies whereby national computer security incident response teams (CSIRTs) are situated under the authority of or report to law enforcement and national security actors risk "seriously hampering cooperation with other CSIRTS", according to the United Nations Internet Governance Forum's Best Practice Forum on establishing CSIRTs for internet security. In addition, assigning law enforcement and surveillance mandates to national CSIRTs would likely reduce international trust and any cooperation sought from other CSIRTs: "When there is a concern of a CSIRT being involved in direct law enforcement or surveillance operations, trust generally tends to be lower than when the CSIRT operates based on information received directly from affected parties".[11]

More generally with regards to their formation if such Cybersecurity Inspectors were established, we note that the Draft Law does not expressly enumerate the required qualifications of Cybersecurity Inspectors. Such qualifications should be precisely identified within the Draft Law to give full clarity to the Cybersecurity Inspectors' specific powers and their remit to discharge their duties.

Further, more clarity is needed in delineating the authority provided under article 26 to Cybersecurity Inspectors to "investigate, observe, monitor, prevent and respond to

---

[8] UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, UN Doc. A/HRC/29/32, 22 May 2015 ("A/HRC/29/32"), para. 32.
[9] CCPR/C/GC/34, para. 34.
[10] A/HRC/29/32, para. 45.
[11] Internet Governance Forum. 2014. "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security," pp. 13, 15, available at https://www.first.org/global/governance/bpf-csirt-2014-outcome.pdf.

cybersecurity threats and […] incidents",[12] in order to comply with the legality principle, which requires laws to not "confer unfettered discretion […] on those charged with its execution."[13] We note that article 26 does not establish the specific measures that Cybersecurity Inspectors are authorized to take to carry out its functions and *when and under what circumstances* Cybersecurity Inspectors may exercise these powers. Any subsequent *Prakas*,[14] pursuant to article 29 to determine the "formalities and procedures of cybersecurity inspection", must clearly and precisely define the specific powers of the Cybersecurity Inspectors, and when and how they may be exercised. The risk of abuse is compounded by the absence of adequate oversight or remedial mechanisms.

**Vague and Overbroad Terms**

*Purpose of measures to respond to cybersecurity threats*

The already overly expansive powers granted to the DSC and Cybersecurity Inspectors risk becoming nearly unfettered given the range of vague and overbroad terms in the Draft Law, inconsistent with the principles of legality and legitimate purpose. Generally, article 3(2) of the Draft Law defines "Managing and Maintaining Cybersecurity" as "any measure or procedure established to prevent, cope with, and mitigate the risk of cybersecurity threats […] which affect national security, economic security, martial security, and public order". Additionally, article 20 of the Draft Law states that a "cybersecurity threat or incident shall be classified as critical" if it may lead to, among others, "a significant harm to the national security, national defence, foreign relations, economy, public health, safety, or public order". This is an extraordinary broad range of areas, covering nearly all aspects of life and goes well beyond a narrow, specific focus on core cyber crimes such as illegal network access or the protection of specifically defined or designated critical information infrastructure, as done in other national cybersecurity and cybercrime laws which seek to advance systemic, user centric, and human rights respecting cybersecurity.[15] These definitions act as the basis for the DSC and Cybersecurity Inspectors to enact measures aimed at protecting these purported aims.

To the extent that the measures may interfere with the exercise of the rights to privacy and freedom of expression, "economic security" and "martial security" do not constitute legitimate purposes to interfere with the enjoyment of these rights.[16] Even where such purposes are for the purported aims of ensuring national security or public order, permitted by international law, the aims must be narrowly defined and subject to strict limitations to ensure limitations on the rights to privacy and expression are necessary and proportionate. Such limitations are not clarified in the law, and provide for a wide scope of executive interpretation and potential abuse. In particular, none of these terms are defined and safeguards to ensure rights violations are not perpetuated are not stated within the Draft Law. These omissions risk granting the authorities unfettered discretion to both interpret and implement measures which are unpredictable and can arbitrarily restrict human rights.[17]

---

[12] Under article 27, the authority of a Cybersecurity Inspector must be exercised "in accordance with regulations of the Code of Criminal Procedure". Under article 29, it is provided that the "[f]ormalities and procedures of cybersecurity inspection shall be determined by Prakas of the Minister of MPTC".

[13] CCPR/C/GC/34, para. 25.

[14] A Prakas is an official proclamation, which is a ministerial or inter-ministerial decision signed by the relevant Ministry or Ministries.

[15] See, for instance, Europe Union Agency for Network and Information Security, "Methodologies for the identification of Critical Information Infrastructure assets and services", December 2014, available at: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/@@download/fullReport or "6 USC CHAPTER 1, SUBCHAPTER XVIII, Part B: Critical Infrastructure Information", available at: https://www.cisa.gov/sites/default/files/publications/CII-Act.pdf.

[16] A limitation on the rights to privacy and freedom of expression and information may only be permissible and non-arbitrary if it serves one of the legitimate purposes of: respect for the rights or reputations of others, national security, public order, public health, or morals. See: ICCPR, art. 19(3).

[17] For example, prior to the 2018 elections, the government issued an inter-ministerial order (*prakas*) to shut down independent media outlets on the basis that the outlets contained content that would "cause social chaos and threaten national security". See: Cambodian Center for Human Rights, 'Cambodian groups seek revocation

*Overbroad and inconsistent definition of "Organizations of CII"*

Our organizations are also concerned that the Draft Law may impose onerous administrative obligations on certain categories of organizations through its broad designation of "Organizations of Critical Information Infrastructure" ("Organizations of CII"). Organizations of CII are obligated to conduct and submit a "risk assessment on its management and maintenance of cybersecurity to its Competent Regulator" (article 13); and "make changes to its systems […] in accordance with recommendations from its respective Competent Regulators" (article 14);[18] notify the Competent Regulator and the DSC of a "cybersecurity threat or cybersecurity incident" within 72 hours, assess the impact of the threat or incident, and "prevent, cope with, and mitigate impacts" (article 16). Any person found guilty of failing to comply with these obligations can face criminal sanctions in the form of heavy fines and potential imprisonment (articles 39 and 40).

In particular, organizations of CII, under article 7, include public and private entities that provide "digital" and "media" services, and other essential services, without further clarification. The draft law also imposes the same administrative requirements for these entities, regardless of size. This may allow "Competent Regulators" to include small and medium enterprises, including small independent online media companies or civil society organizations with online platforms as organizations of CII, who may not have the capacity to meet the corresponding administrative requirements, including installing and maintaining costly network security measures.[19] If these small and medium entities fail to meet such onerous requirements, they may face punitive criminal sanctions, as indicated below, which may constitute an impermissible restriction on the right to freedom of expression and information. We also note that the Draft Law is inconsistent on the definition of "Critical Information Instructure", which may result in contradictory designations of organizations of CII: article 3(20) uses the phrase "infrastructures in the public interest" rather than the phrase "essential services" used in article 7.

**Unnecessary and Disproportionate Criminal Sanctions for Non-Compliance**

The imposition of criminal sanctions for non-compliance, including heavy fines and imprisonment, is inconsistent with the principles of necessity and proportionality, as they are not the least restrictive means to sanction or regulate the conduct of individuals who fail to comply with the obligations established by the Draft Law.[20] These sanctions as they currently stand will risk disproportionate rights violations towards the existing vaguely-defined aims of the Draft Law – in net effect, causing more damage to Cambodian society than benefit.

Article 39 of the Draft Law imposes a fine between KHR50,000,000 (approx. USD 12,000) to KHR80,000,000 (approx. USD19,000) upon any person who does not conduct a risk assessment. If the same person commits the same offense within one year, then the offender will be punished with "imprisonment from 6 (six) months to 1 (one) year and fined double the amount". Such sanctions are particularly disproportionate when applied to small media outlets that do not intend to cause harm and may fail to comply due to the lack of capacity to meet the onerous administrative obligations. The Draft Law also imposes heavy fines and imprisonment for failing to "cooperate with a DSC official responsible for cybersecurity or

---

of new online directive ahead of elections', IFEX, 15 June 2018, Available at: https://ifex.org/cambodian-groups-seek-revocation-of-new-online-directive-ahead-of-elections/.

[18] "Competent Regulator refers to any ministry or institution having roles and duties related to management and maintaining cybersecurity of CIIs under its respective jurisdiction" (article 3(14) of the Draft Law).

[19] An example of overly onerous administrative requirements being used to curtail media freedom was when the independent newspaper – The Cambodia Daily – was forced to shut down after the government imposed a USD6.3 million tax bill for alleged tax evasion. Richard Paddock, *"The Cambodia Daily to Close (After Chasing One Last Big Story)",* The New York Times, 3 September 2017, available at: https://www.nytimes.com/2017/09/03/world/asia/cambodia-daily-newspaper.html.

[20] CCPR/C/GC/34, para. 34.

Cybersecurity Inspector" (article 42) or opposing "the performance of the duties of the DSC or MPTC" (article 44). This risks threatening the right to privacy and creating a chilling effect on the right to freedom of expression, as private organizations are forced to comply with any decision taken by the DSC and Cybersecurity Inspectors to avoid being held liable.

**Absence of Independent Oversight and Inadequate Access to Effective Remedy**

The potential for abuse arising from the overly expansive powers being granted to the DSC and Cybersecurity Inspector is compounded by the absence of any independent or impartial oversight mechanism, judicial or administrative, over the exercise of executive powers enumerated under the Draft Law. There is also a clear lack of a meaningful right to appeal or access to effective remedy for affected individuals or organizations. Under article 2(3) of the ICCPR, Cambodia is obligated to ensure the right to an effective remedy for a violation of human rights,.[21] Although article 30 of the Draft Law grants the right to challenge any decision taken by a DSC official or a Cybersecurity Inspector, there are procedural hurdles to meaningfully access the right to appeal.

The initial stage of redress available to an aggrieved party who "does not agree with any measure" is not an appeal to the courts, but an administrative appeal within 30 days of receiving notice of the measure (article 30) to the Minister of Post and Telecommunications, who coordinates the DSC and Cybersecurity Inspectors. This results in a self-checking process still embedded in executive control. If the person does not agree with the decision of the Minister, they can then file a complaint to the competent courts. However, any complaint to the courts "may not effectively halt the implementation of the decision of the Minister of the MPTC". This may render the appeal process altogether ineffective because irreversible damages may arise during the time of filing a complaint to the court, such as when the DSC has gained access to data stored on a "computer or computer system" when exercising its authority under article 21(1) of the Draft Law. The Draft Law is silent as to how such damages or related rights harms will be remedied in such an event.

**Recommendation**

In light of these concerns, we recommend that the Cambodian authorities withdraw or substantially amend the Draft Law, to ensure compliance with Cambodia's international human rights obligations to respect the rights to privacy and freedom of expression and information, and to advance cybersecurity that better protects individuals and organizations. Amendments to the Draft Law must significantly address concerns relating to unfettered powers granted to the executive; vague and overbroad provisions allowing for executive overreach and abuse; overbroad prohibitions on providing cybersecurity services unless specifically licensed by the executive; unnecessary and disproportionate sanctions for non-compliance and the absence of any independent or impartial oversight or remedial mechanism and access by individuals and organizations to effective remedies.

[21] A/HRC/29/32, para. 19. See also: Human Rights Committee, *General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant*, UN Doc. CCPR/C/21/Rev.1/Add.1, 26 May 2004, para. 15.