ICNL

www.icnl.org
info@icnl.org

Legal Analysis: CAMBODIA

Draft Law on Cybercrime, 2024

Introduction

Cambodia is currently considering a draft "Law on Cybercrime" ("draft law"). The law aims to deter, prevent, and suppress cybercrimes. At the request of partners, ICNL is pleased to share an analysis of the draft law, focusing on recommendations to revise the law to better protect the freedom of expression, right to privacy, and other civic space concerns.

While the draft law contains some commendable processes, such as requiring court orders for some forms of access to computer systems and data, as well as protecting the right to appeal decisions on cybercrime issues to the Minister of Interior and ultimately to a court, it also contains several provisions that do not comply with international law. These include:

- **Restrictions to the freedom of expression**
    - The criminalization of intimidation, threat, abuse, and insults of another person, which could limit criticism of authorities and government policies;
    - The criminalization of defamation, which could restrict criticism of public figures; and
    - The criminalization of communicating false information, which could silence critics of authority figures and their policies.
- **Restrictions to the right to privacy**
    - Overbroad search and seizure powers of judicial police officers, which could grant authorities significant surveillance powers;
    - Unlimited extensions of traffic and content data, which could grant authorities powers to surveil civil society and other individuals beyond the investigation of a crime;
    - Overbroad powers to distribute data, which could grant authorities discretion to surveil civil society and other individuals; and
    - The lack of explicit protection of whistleblowers, who are essential to furthering the public's right to access information in the public interest.

This analysis compares the draft law to international law, standards and best practices related to the freedom of expression, right to privacy and other relevant civic freedoms. It does not address every issue within the draft law.

International Law

Right to freedom of expression: Article 19 of the International Covenant on Civil and Political Rights (ICCPR) 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]

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 protects the right to privacy. The protection of the right to privacy is essential to the full realization of the right to freedom of expression; undue interference with individuals' privacy can have a chilling effect on their willingness to develop, exchange, and access ideas.[4] Any limitations on the right to privacy must also pass the three-part test noted above, where the legitimate purposes for restricting the right to privacy are to protect national security, public order, public health or morals, and the rights and freedoms of others.[5]

Issues

CRIMINALIZATION OF INTIMIDATION, THREAT, ABUSE, AND INSULTS OF ANOTHER PERSON

ISSUE: Article 42's prohibition of intimidating, threatening, or abusing another person[6] and Article 44's prohibition of using insulting, derogatory or rude language[7] impermissibly restrict

[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.
[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] See United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the freedom of opinion and expression, Frank La Rue*, A/HRC/23/40 (2013), Part A ("Interrelations between the rights to privacy to freedom of opinion and expression").
[5] See *id.* at Part B ("Permissible limitations to privacy and freedom of expression").
[6] Draft law. Article 42 on information technology-related abuse makes it a crime to intentionally cause "intimidation, threat, or abuse to another person by information technology-related means."
[7] Draft law, Article 44 on insults criminalizes "the use of any insulting, derogatory or rude language without imposing blame on any act through information technology."

the freedom of expression. These are overly broad limitations on the freedom of expression that could restrict criticism of the government or its policies.

ANALYSIS: While governments may have a legitimate interest in regulating harassment online, restrictions to the freedom of expression are lawful only when they pass Article 19's three-part test. The terms "intimidate," "threat[en]," "abuse," "insulting," "derogatory," and "rude" are not sufficiently precise as to allow a person to understand what speech or behavior is prohibited, thus failing the principle of legality. Additionally, international law protects even "deeply offensive" or insulting speech.[8] Article 44 appears to criminalize even mildly insulting speech in violation of this standard.[9]

Without further definition of these terms, authorities have broad discretion to determine that a person has intimidated, threatened, abused, or insulted someone. For example, an authority might arrest opposition party members, civil society, or private individuals for calling for the resignation of government representatives by interpreting the calls as intimidation or threats. Applying the law in this way would result in a silencing of opposition and other critical voices. One way to narrow the scope of the provisions is to make these actions a crime if they directly lead to significant physical or emotional harm of a person.

International law requires that public figures tolerate a greater degree of criticism than private citizens.[10] The United Nations Human Rights Committee explains that "the mere fact that forms of expression are considered to be insulting to a public figure is not sufficient to justify the imposition of penalties," and explicitly notes that "all public figures…are legitimately subject to criticism and political opposition." The draft law should include language to prevent authorities from using these provisions to silence criticism of public figures.

RECOMMENDATION: Amend Article 42 to make it a crime if the intimidation, threat, or abuse directly leads to a significant physical or emotional harm. At the end of Article 42, insert a clause that explicitly allows for the criticism of government officials, government policies, and other public figures. Remove Article 44.

CRIMINALIZATION OF DEFAMATION

ISSUE: Article 43 criminalizes online defamation.[11] The criminalization of defamation could likewise silence dissent and constitutes an impermissible restriction on the freedom of expression.[12]

ANALYSIS: States should strongly consider the decriminalization of defamation and only apply criminal law against the most serious cases of defamation.[13] Imprisonment as a penalty for

[8] General Comment No. 34, supra note 2, at para. 11.
[9] It should be noted that Section 2 of Cambodia's Criminal Code already criminalizes insults made in a public space or public platform. It is therefore unclear why Article 44 of the draft law is necessary since this type of speech is already prohibited (though likely in contradiction of international law).
[10] See General Comment 34, supra note 2, at para. 38. See also United Nations Economic and Social Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. Abid Hussain, submitted in accordance with Commission resolution 1999/36*, E/CN.4/2000/63 (2000), p. 18.
[11] Draft law, Article 43 criminalizes an "exaggerated claim or insincere blame for any act that harms the honor or reputation of an individual or institution."
[12] It should be noted that Cambodia's Criminal Code in Articles 305-06 already defines defamation as an offense, including defamation through the media. It is therefore unclear why Article 43 of the draft law is necessary. As explained in the analysis, both these offenses would likely contradict international law.
[13] General Comment No. 34, supra note 2, at para. 47.

defamation fails the principle of proportionality because it is not the least restrictive means to protect the reputation of a person. A less restrictive means would be to apply civil penalties in defamation cases; these could include allowing a court to order the offender to issue a correction of false information or to pay a fine to compensate the victim in case there is a measurable harm. The range of permissible fines in the draft law should match that of the offense of defamation under the Criminal Code (i.e., one hundred thousand to ten million Riels rather than two million to twenty million riels).[14]

The risk of imprisonment and other criminal penalties for defamation under the draft law could have a silencing effect on individuals because they fear that authorities would apply significant penalties in retaliation for voicing criticism. To limit the risk that authorities abuse defamation laws to silence critics, where states make defamation a punishable offense, the law should explicitly allow for the accused person to make the defense that she/he made reasonable efforts to ascertain the truth of a matter that was in the public interest.[15] For example, the European Court of Human Rights held that a newspaper and its editor should not be held liable for defamation despite publishing false statements that members of a seal hunting vessel had committed criminal acts because they had acted in good faith by reporting on a matter of public interest that was supported by a report issued by the Ministry of Fisheries, which had a high degree of credibility.[16] Defamation should also not be applied to forms of expression that are not typically subject to verification, such as an opinion editorial as opposed to an article reporting on a recent event. Furthermore, the offense of defamation should require as an element that the accused made the statement with intent to harm the honor or reputation of an individual.[17]

Finally, public bodies should not be able to bring defamation actions.[18] Similarly, under international law, it cannot be a crime to defame objects and symbols. Objects and symbols, unlike people, do not have a "reputation" to defend though defamation laws. The purpose of defamation laws is to protect the reputations of individuals and not to prevent criticism of the government, other authorities, or concepts.[19]

RECOMMENDATION: Remove Article 43 since defamation is already an offense under the Criminal Code. If Article 43 is retained in the draft law, remove imprisonment as a penalty for defamation and instead state that a court may order the accused to issue a correction of a false statement or to pay a fine of one hundred thousand to ten million Riels, depending on

[14] See Criminal Code, Article 305.
[15] General Comment No. 34, supra note 2, at para. 47. United Nations Economic and Social Council, *Civil and Political Rights Including the Question of Freedom of Expression* (January 2000), E/CN.4/2000/63, available at https://documents.un.org/doc/undoc/gen/g00/102/59/pdf/g0010259.pdf?token=oj63GMbuve9pIZqvgV&fe=true,, paras. 51-52. An issue is in the public interest if it relates to public figures and public officials, politics, public health and safety, law enforcement and the administration of justice, consumer and social interests, the environment, economic issues, the exercise of power, and arts and culture. Article 19, Defining Defamation: Principles on Freedom of Expression and Protection of Reputation (July 2000), available at https://www.article19.org/wp-content/uploads/2018/02/defining-defamation.pdf, footnote 9.
[16] See European Court of Human Rights, Bladet Tromso and Stensaas v. Norway, Application No. 21980/93 (May 1999). For a summary of the case, see Columbia University, "Bladet Tromso and Stensaas v. Norway," available at https://globalfreedomofexpression.columbia.edu/cases/bladet-tromso-and-stensaas-v-norway/.
[17] See, General Comment No. 34, supra note 2, at para. 47.
[18] United Nations Economic and Social Council, *Civil and Political* Rights, supra note 15, at para. 50.
[19] Id. at para. 52. See also United Nations General Assembly, *Promotion and protection of the right to freedom of opinion and expression* (September 2016), A/71/373, para. 41 (explaining that the freedom of expression protects individuals holding or expressing beliefs, rather than the belief or belief system itself).

the severity of the harm caused by the statement. Also, add in defenses to the crime of defamation, including if the accused made reasonable efforts to ascertain the truth about a matter in the public interest. Finally, require that the "exaggerated claim or insincere blame" under Article 43 is issued with malice or in bad faith.

CRIMINALIZATION OF COMMUNICATING FALSE INFORMATION

ISSUE: Article 49 prohibits communicating false information that intentionally harms a range of public interests grants the government broad discretion to determine that a person has shared prohibited information.[20] This provision could have a silencing effect on civil society and the broader public.

ANALYSIS: Criminalizing the dissemination of false information is incompatible with international standards for restrictions on the freedom of expression and should be abolished.[21] Laws that restrict "false" content could stifle independent media, chill public debate, and undermine government and public accountability where critical views are deemed false.

Article 49 of the draft law is not a permissible restriction on the freedom of expression under international law. The provision fails the principle of legality because the term "false information" is not clearly defined, making it difficult for a person reading the law to understand when a statement may be considered "false." Likewise, it is unclear from the provision when a statement might "harm national defense, national security, relations with other countries, economy, public order, or causes discrimination, or affects traditional culture…" This ambiguity grants authorities broad discretion to determine that a person has published "false" information that affects the public interest and therefore has committed an offense under the draft law. For example, if an economist shares research that Cambodia's Gross Domestic Product (GDP) will grow by 5% in the next year but Cambodia's Ministry of Economy and Finance reports that the GDP will grow by 7%, authorities could claim that the economist has intentionally published "false" information to harm Cambodia's economy in violation of the draft law. This interpretation of the provision could lead to a decrease in independent research on issues related to Cambodia.

Article 49 also fails the principle of proportionality because criminalizing false information is not the least restrictive means to protect a legitimate public interest. For example, an alternative and less restrictive way to protect the rights and reputations of others would be to use civil defamation law rather than criminal measures to curb false information such as defamation; civil defamation law could provide for penalties such as apologies, corrections, and damages to the person injured by the publication of false information.

---

[20] Draft law, Article 49 subject "any person who disseminates or distributes false information through information technology that intentionally harms national defense, national security, relations with other countries, economy, public order, or causes discrimination, or affects traditional culture" to punishments including imprisonment of three to five years and a fine.

[21] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*, FOM.GAL/3/17 (2017), para. 2(a).

From a policy perspective, criminalizing "false" information, like in Article 49, will: (a) stifle independent media, especially those outlets and reports that are critical of government policies; (b) create a chilling effect on public debate; (c) undermine government and public accountability because the presentation of critical views is criminalized; (d) result in less information on community needs being available to government decision-makers, thereby impeding government ability to solve problems; and (e) weaken democracy. Ironically, laws seeking to prohibit false news may actually result in the suppression of "true news," including the presentation of non-partisan, objective analysis, especially where such analysis challenges a government policy or position.

RECOMMENDATION: Remove Article 49.

OVERBROAD SEARCH AND SEIZURE POWERS

ISSUE: Under Article 14(1), a judicial police officer can request a court to provide an order to search or access a computer system or data within a computer system without meeting a minimum threshold for believing that the computer system or data contains evidence of a crime.[22]

ANALYSIS: This provision allows a judicial police officer to seize computers or data storage systems, make and retain a copy of computer data, and make the data inaccessible or remove it from the computer system. These powers would disrupt the operation of civil society organizations (CSOs), private businesses, universities, amongst other entities, and would grant judicial officers access to sensitive information about the activities, staff, members, donors, partners, or investors of these entities without a minimum degree of belief that it or its associated personnel are involved in criminal activities.

To safeguard against the abuse of power to surveil individuals and organizations, including civil society, the draft law should set a standard of proof, such as "probable cause," for competent authorities to access computer systems or data. The draft law already requires judicial officers to have "reasonable grounds to believe" that the access to a computer system or data sought is evidence of a crime or related to a person under investigation of a crime in several provisions.[23] However, "reasonable grounds" is low threshold to satisfy and amounts to a *de facto* approval of law enforcement requests.[24] Adopting the "probable cause" standard would offer greater protections against undue surveillance. Countries like the United States have adopted a probable cause threshold for electronic surveillance.[25]

Article 14(1) should also be revised to guarantee procedural safeguards for search and seizure prescribed under international law. These include the requirement to obtain a court-issued warrant based on probable cause of an infraction of the law before search and seizure, with

[22] Draft law, Article 14(1) states "In order to search or gather the evidence necessary for a criminal investigation in which a computer system or a computer data storage medium may contain evidence of that crime, the judicial police officers shall request a court to:
- Search or access a computer system or part of it and computer data stored therein;
- Search or access a computer or data storage medium in which computer data may be stored; and
- With such assistance as may be necessary using existing technical capability."

[23] See, for example, Draft law, Articles 12(1), 13(1), 15(1), and 16(1).

[24] *Report of the Special Rapporteur*, supra note 4, at para. 56.

[25] Cornell Law School Legal Information Institute, "electronic surveillance," available at https://www.law.cornell.edu/wex/electronic_surveillance#:~:text=To%20obtain%20a%20warrant%2C%20the,the%20surveillance%2C%20among%20other%20requirements.

details on the material that will be surveilled directly related to the crime being investigated, limits on the duration of the warrant, and requirements to destroy the material seized following the conclusion of the investigation.[26, 27]

RECOMMENDATION: In Article 14(1), require a judicial police officer to have "probable cause" to believe that a computer system or computer data storage medium contains evidence of a crime before requesting a court to issue a warrant for search and seizure. The warrant must be based on a reasonable suspicion of an infraction of the law, clearly describe the surveilled material which must be directly related to the crime being investigated, limit the duration of the surveillance, and require the destruction of the material seized after the investigation concludes. Consider establishing an independent body that approves and reports on all government surveillance activities.

UNLIMITED EXTENSIONS OF ACCESS TO TRAFFIC AND CONTENT DATA

ISSUE: Articles 15(2) and 16(2) seem to enable judicial police officers to request unlimited extensions for collecting traffic data[28] (i.e., data related to the routing, timing, and duration) and intercepting content data, respectively.[29] This could result in extended surveillance of civil society and the public, which limits privacy rights and could impinge on civic freedoms.

ANALYSIS: Under international law, laws authorizing the surveillance of peoples' electronic data or communications must include safeguards on the nature, scope, and duration of surveillance measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.[30] These safeguards include strict time limits on the surveillance measures. The German approach is instructive here: a court may issue a warrant to surveil/intercept traffic or content data for up to 180 days and can then issue one extension for up to 180 days, but only if the conditions for warrant continue to exist.

By allowing a court to extend a surveillance order "for a further specific period," Articles 15(2) and 16(2) do not set a firm end date for the surveillance extension. A court could interpret the provision to extend an order by several months, years, or indefinitely. Without limitations on

---

[26] *Report of the Special Rapporteur*, supra note 4, at para. 81. *See also*, United Nations Human Rights Council, *The right to privacy in the digital age*, A/HRC/27/37 (2014), available at https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf, paras. 37-38, *and* United Nations Human Rights Council, *Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/41/35 (2019), para. 52.

[27] To better protect privacy rights while still enabling surveillance for law enforcement, governments have begun adopting a mixed model of judicial, parliamentary, and public oversight. For example, the city of Oakland in California, adopted a surveillance technology purchase approval process that is carried out by relevant authorities, issues public notice of surveillance technology purchases, and issues regular public reporting on approvals, purchases, and uses of surveillance technology.

[28] Draft law, Article 15(2) permits a court to authorize an extension "for a further specified period" of a previous order to a service provide to collect, record, and provide traffic data about specified communications to a judicial police officer where there are reasonable grounds to believe that the traffic data is required in an investigation of a crime.

[29] Draft law, Article 16(2) permits a court to authorize an extension "for a further specified period" of a previous order to a judicial police officer or a service provider to collect or record content data where there are reasonable grounds to believe that the content data is related to an investigation of a crime.

[30] Report of the U.N. Special Rapporteur, A/HRC/23/40, supra note 4, at para. 81. See also, Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/41/35, supra note 26, at para. 50.

the duration and requirements for grounds of the extension, judicial police officers might request access to traffic and content data for undefined periods and without clear limitations on how they are using the data. These powers limit the right to privacy. Judicial police officers might secure court orders to continue surveilling CSOs, individuals, or private companies even after an investigation concludes. The judicial police officers could interfere with a CSO, private citizen, or private company's activities by using information gained from surveillance to disrupt a planned protest or other legal activities.

Both Articles 15(1) and 16(2) limit the original court ordered period of surveillance to 14 days and require the judicial police officer to demonstrate reasonable grounds to believe that the traffic data and content data respectively are related to an investigation of a crime. Adjusting Articles 15(2) and 16(2) to adopt a limited period for extensions (such as 180 days) and clarify the grounds for the extension would help safeguard against abuse of power to surveil CSOs and individuals beyond investigation of a crime.

RECOMMENDATION: Revise Articles 15(2) and 16(2) to limit extensions of court orders to a maximum of 180 days and require the judicial police officer to demonstrate reasonable grounds to believe that continued access to traffic data and content data would be related to an investigation of a crime.

OVERBROAD POWERS TO DISTRIBUTE DATA

ISSUE: Article 26 states that competent officers may distribute data about a person under investigation if the officer has "lawful authorization, excuse or justification."[31]

ANALYSIS: Any interference with the right to privacy, such as through surveillance, must be authorized through laws that ensure the collection of data are tailored to specific legitimate aims and are sufficiently precise and specify in detail the precise circumstances in which any interference is permitted.[32] For example, in the draft law, authorities should be obligated to protect intercepted data and limit their sharing or usage of the data to furthering an investigation or prosecution of an alleged crime.

Although Article 26 makes it an offense for a competent officer to distribute data about a person under investigation unless the officer has lawful authorization, excuse, or justification, the article is too broad to comply with international law.

The provision fails the principle of legality because it is impossible for a competent officer to understand when an "excuse of justification" would allow the sharing of a person's data. These terms are so vague that they grant a competent officer to determine that it is necessary to share a person's data. These powers raise privacy concerns: a competent officer could share sensitive information about a CSO's staff, members, beneficiaries, or donors while the CSO is under investigation because he believes the public should be wary of the CSO and its associated personnel. This kind of "excuse or justification" could expose civil society and other actors to retaliation by authorities.

[31] Draft law, Article 26 states that "any competent officer under this law who intentionally, without lawful authorization, excuse or justification, distributes computer data, traffic data, or other data of the person under investigation shall be punishable by imprisonment…and a fine…"
[32] *The right to privacy in the digital age*, A/HRC/27/37, supra note 26, at para. 28.

RECOMMENDATION: In Articles 26, remove "excuse or justification" as grounds for a competent officer to share a person's data.

PROTECTION OF WHISTLEBLOWERS

ISSUE: Article 34 allows any person to access a computer system[33] and Article 36 allows a person to intercept data[34] if the person has "lawful authorization, excuse or justification." These articles may be intended to protect security researchers or experts to test public and private organizations' computer systems, which they do. However, the provisions should be expanded to explicitly protect whistleblowers as well.

Additionally, Article 35 criminalizes the access of a computer system beyond the parameters of a person's authorized access to the system,[35] which could be interpreted to prohibit whistleblowers who access a computer system in an unauthorized way.

ANALYSIS: The freedom of expression protects whistle-blowers, who further the public's right to receive information that is in its interest.[36] Laws should protect whistle-blowers, who are persons who expose information that they reasonably believe to constitute a threat or harm to a specified public interest, such as a violation of national or international law, abuse of authority, waste, fraud, or harm to the environment, public health, or public safety.[37] Whistle-blower laws should protect whistleblowers even if they blow the whistle on those outside of a work-based relationship.[38] In addition to protecting security professionals, Articles 34 and 36 would appear to protect whistle-blowers, who may access a computer system or intercept data to share information that might harm the public interest, even if they do not have legal authorization to do so. These provisions should be revised to explicitly protect persons who access or intercept data that they reasonably believe to constitute a threat or harm to a specified public interest.

Conversely, Article 35 appears to prohibit whistleblowers from accessing a computer system without authorization. This provision should be revised to add an exception for persons who access a computer system in an unauthorized way to share information that constitutes a threat or harm to a specified public interest and do not harm the underlying computer systems or its data.[39]

RECOMMENDATION: Revise Articles 34 and 36 to explicitly protect persons who access or intercept data that they reasonably believe to constitute a threat or harm to a specified public

[33] Draft law, Article 34 states that "any person who intentionally, without lawful authorization, excuse or justification, accesses the whole or any part of a computer system shall be punishable by…imprisonment…and a fine…"
[34] Draft law, Article 36 states that "any person who intentionally, without lawful authorization, excuse or justification, intercepts data transferred to, from, or within a computer system by any means shall be punishable by…imprisonment…and a fine…"
[35] Draft law, Article 35 states that "Any person who is authorized to access the whole or any part of a computer system but who obtains, copies, uses and/or transfers computer data or information of the owner without authorization shall be punishable by…imprisonment…and a fine…"
[36] United Nations General Assembly, *Promotion and protection of the right to freedom of opinion and expression: Note by the Secretary-General*, A/70/361 (2015), para 5.
[37] Id., at para. 28.
[38] Id., at para. 29.
[39] See e.g., The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, Joint Declaration December 6, 2004, p. 4 (2004).

interest. Revise Article 35 to add an exception for persons who access or intercept data that they reasonably believe to constitute a threat or harm to a specified public interest.

OTHER ISSUES

The draft law contains several other issues which may impact Cambodian internet users:

- Article *2* creates universal jurisdiction. The Law's scope is outlined in Article 2 as being "applicable to any cybercrime committed within or outside the territory of the Kingdom of Cambodia, which in any way infringes the security, public order or interests of the Kingdom of Cambodia."[40] This creates universal jurisdiction over every internet user, which is problematic for two main reasons. First, many internet users, especially those outside of Cambodia, will not be aware of this Law or its applicability. Second, the categories of offenses listed, those that "infringe the security, public order, or interests of the Kingdom of Cambodia," are so broad that nearly any discussion of Cambodia that includes negative attributes or any criticism could be categorized as an offense.
- Article 22 allows persons who violate the draft law to pay "a transitional fine" which will "extinguish criminal actions." Allowing persons to pay a fine to "extinguish" the criminal charge discriminates against less affluent persons who may be unable to pay the transitional fine and therefore must bear imprisonment as a penalty to violating the draft law. This provision should be removed.
- Article 24 allows a legal entity to be declared criminally liable for an offense committed by an organization or its representative "for the benefit of that legal entity." The provision explicitly cites Article 42 of the Criminal Code, which describes the criminal responsibility of legal entities. Article 24 of the draft law should mirror the language in the Criminal Code, which allows legal entities to be held criminally responsible "for offences committed on their behalf by their organs or representatives." The current text ("for the benefit of that legal entity") is overly broad and could render legal entities liable for actions taken by persons who are not their representatives.
- Article 32 prohibits the advertisement and mobilization of funds for purchase, sale, exchange or payment transactions of cryptocurrency without authorization or license from the competent authority.[41] Cryptocurrency is a well-recognized method for payment used by businesses, governments, civil society organizations and individuals. Rather than issuing criminal sanctions for offering payment in cryptocurrencies, the RGC should create a regulatory framework that enables such payments to be conducted in a clear, transparent manner.
- The definition of pornography under Article 3(16) is broad and could be interpreted to prohibit works of artistic expression. Cambodia has used a similar provision under its criminal code to target women who wear "revealing" clothing[42] and has previously

[40] Draft law, Article 2.
[41] Draft law, Article 32 states that: Cryptocurrency: "Any person who advertises and mobilizes funds for purchase, sale, exchange or payment transactions of cryptocurrency via information technology without authorization or license from the competent authority shall be punishable by… imprisonment… and a fine …."
[42] See, e.g., Amnesty International, "Cambodia: Drop discriminatory

proposed laws banning "inappropriate" dress.[43] The government could use the ban on pornography under this draft law to target women activists. For example, the government could claim that a female activist is engaging in pornography if she is dressed in more revealing clothing in an online campaign. Such an interpretation could limit the freedom of expression, especially that of women in the public eye, who are often targeted with criticism about their sexuality.

Moreover, the penalty for pornography under the draft law should match the penalty for the comparable crime under existing laws. Article 249 on indecent exposure in the Criminal Code subjects a perpetrator to six days to three months of imprisonment and a fine of between one hundred thousand to five hundred thousand Riels. Article 39 of the Law on Suppression of Human Trafficking and Sexual Exploitation punishes persons who distributes pornography to seven days to one month of imprisonment and a fine of between one hundred thousand to two hundred thousand Riels; a person who produces pornography is subject to one month to one year of imprisonment and a fine of between two hundred thousand to two million Riels. The penalties for pornography, especially the fines, are much higher in the draft law: imprisonment between 1 to 6 months and a fine between ten million and twenty million Riels.

Conclusion

ICNL appreciates the opportunity to analyze the draft Cybercrimes law. Revising the issues highlighted in this analysis would bring the law into greater compliance with international law on the freedom of expression. ICNL remains available to provide technical assistance, as appropriate. For further information or queries, please contact ICNL's Digital Rights Team (digital@icnl.org).

Pornography charges against Facebook seller," (February 21, 2020), available at https://www.amnesty.org/en/latest/news/2020/02/cambodia-drop-discriminatory-pornography-charges-against-facebook-seller/.

[43] Voice of America Cambodia, "Women, activists decry decency clauses in draft public order law," (August 5, 2020), available at https://www.voacambodia.com/a/5531328.html.