



ចក្ខុវិស័យមនុស្សកម្ពុជា
Cambodian Center for Human Rights

Legal Impacts on Freedom of Expression in the Digital Age

November 2025



Cambodian Center for Human Rights

The Cambodian Center for Human Rights (“CCHR”) is a non-aligned, independent, non-governmental organization (“NGO”) that works to promote and protect democracy and respect for human rights – in particular civil and political rights – throughout the Kingdom of Cambodia (“Cambodia”). CCHR’s vision is of a peaceful Cambodia in which all people can enjoy the fundamental human rights to which they are entitled, all are subject to the rule of law without impunity, all are treated equally without discrimination, all are empowered to participate fully in the democratic process, and all can share in the benefits of Cambodia’s sustainable economic development. CCHR’s logo – a dove flying in a circle of blue sky – represents the twin principles of peace and freedom.

For more information, please visit www.cchrcambodia.org

About this legal Analysis Paper

This legal analysis paper is an output of CCHR’s Sustaining Independent Media and Fundamental Freedom in Cambodia (“FoEx”) project. The FoEx project, initially launched in September 2020, aims to create a widened space for freedom of expression and a pluralistic and independent environment for free media and to enhance opportunities for citizens to engage and participate in democratic processes and make informed decisions.

This legal analysis paper provides an updated assessment of both existing and draft legislation and legal frameworks in Cambodia that have or may have an impact on freedom of expression in the digital age. It analyses their contents and reach, and the extent to which they adhere to or contravene international human rights law and standards related to freedom of expression, access to information and the right to privacy. The FoEx project has also produced four annual reports, released in [April 2022](#), [November 2022](#), [November 2023](#) and [November 2024](#), respectively.

They can all be found on CCHR’s website:
<https://www.cchrcambodia.org/en/publications/general-reports>.

Queries and feedback

Should you have any questions or wish to provide feedback on this report, please email CCHR at info@cchrcambodia.org. This report, along with all other publications by CCHR, is available online on CCHR's website, www.cchrcambodia.org, or on the award-winning Cambodian Human Rights Portal, www.sithi.org, which is hosted by CCHR.

Alternatively, please contact CCHR at:

#798, Street 99, Sangkat Boeng Trabek, Khan Chamkarmon,
Phnom Penh, Cambodia. Telephone: +855 (0) 23 72 69 01

Table of Contents

Scope and methodology	1
Executive summary	2
Introduction	4
I. Overview of the right to freedom of expression	6
II. Existing legal framework and legislation impacting the enjoyment of the right to freedom of expression online	10
a) Criminal code	
b) Law on the press	
c) Telecommunications law & prakas on social media & website control	
d) Charter for professional journalism & journalist ID cards	
e) Sub-Decree on national internet gateway (NIG)	
III. Draft legislation and policies impacting enjoyment of the right to freedom of expression, access to information and privacy online	23
a) Draft cybercrime law	
b) Draft law on access to information	
c) Draft law on cybersecurity	
d) Draft law on personal data protection	
Conclusion and recommendations	35

Scope

This legal analysis focuses on emerging legislation and standards related to digital freedom of expression in Cambodia under international human rights law, and compares Cambodian laws and legal frameworks to international human rights law and standards, in terms of both consistency and contradiction. It will also provide recommendations in order to ensure the consistency of the relevant laws with international human rights law and standards.

Methodology

This analysis relies on desk-based, comparative research and analysis of Cambodian and international law related to freedom of expression in the digital age. It focuses in particular on existing challenges regarding legal implementation, vagueness of the law and inconsistency between Cambodian law and international human rights law.

Executive Summary

This Legal Analysis assessed the extent to which existing legislation and legal provisions are used to restrict freedom of expression in the digital era, before then assessing the same for a number of pieces of draft legislation which, to differing extents, look set to have the same effect. The picture that emerged from this analysis is one in which draft legislation in the pipeline has the potential to exacerbate the increasingly restrictive environment for freedom of expression in Cambodia.

Assessment of existing legal provisions and legislation underscored that both in their formation and application, they serve to undermine the enjoyment of the right to freedom of expression. Articles of the Criminal Code – specifically 305 (Defamation), 494 & 495 (Incitement), 307 (Public Insult), 523 (the questioning of a judicial decision), and 502 (Insult of a Public Official) – are some such examples, which overwhelmingly do not meet the legality test in international human rights law. The 1995 Law on the Press restricts rather than facilitates or enables media freedom, as such laws are commonly intended to do. It not only imposes restrictions on content but also leaves many scenarios open to interpretation, due to imprecision in wording. The Law on Telecommunications (2015) and the Inter-Ministerial Prakas No. 170 on Social Media and Website Control (2018) are wide-ranging in their powers, granting them disproportionate reach, yet imprecise in the formulation of many of their provisions. The situation for media freedom, already weakened through the Press Law, is made even more vulnerable through the passage of the Charter for Professional Journalism and Journalist ID Cards. The surveillance, interception, and censorship of internet activity are provided for under the Sub-Decree on the National Internet Gateway (NIG), which, despite being set to be enforced from February 2022, has faced significant delays regarding its implementation.

Analysis of draft legislation revealed similar concerns regarding the lack of precision in the formulation of various articles, thus leaving the legislation vulnerable to application for the purpose of self-interest or in pursuit of political aims. The Draft Cybercrime Law is particularly concerning, as it includes harsher penalties – such as imprisonment – for crimes that already exist in the Criminal Code, but do not include such penalties. This may therefore represent an attempt to make the criminalization of freedom of expression even harsher than it already is.

The draft law on Access to Information, despite having a consultative drafting process, contains blanket provisions that present significant barriers to access to information. Significant power regarding the governance of digital security is granted to an executive body, to be called the Digital Security Committee (DSC), as well as to Cybersecurity Inspectors, creating concerns that this will lead to overreach.

Nonetheless, despite these concerns, as the abovementioned pieces of legislation remain in the draft stage, there is still the opportunity to amend them and ensure they are compliant with Cambodia's obligations under international human rights law. Similarly, since August 2024, the Royal Government of Cambodia ("RGC") has undertaken a review of the Criminal Code, which presents an opportunity for reforming the above-mentioned provisions to be amended and brought in line with international human rights law.

Introduction

As is the case the world over, the emergence of digital technology in Cambodia has had a profound impact on how the right to freedom of expression is exercised. Given that digital technology has diffused so many aspects of our daily lives, particularly how we communicate with one another and wider society, this right is now arguably exercised almost equally as much online as it is offline.

As of early 2025, there were 12.9 million social media user identities in Cambodia, equating to 72.4 percent of the total population.¹ When digital technology such as social media, messaging platforms and blogs first emerged in Cambodia, individuals could express themselves online with relatively little self-censorship and without fear of State surveillance or monitoring. These new digital platforms provided alternative options for the public to engage with wider society and express their thoughts, subsequently enlarging the space for freedom of expression. They also allowed the public to express their views on Government policy and decision-making, at times to great positive effect. One such example was the public outcry in 2022 against the Royal Government of Cambodia's (RGC) land concession of Tamoa Mountain to a private company. Ultimately, the RGC overturned its decision to implement the land concession, citing the public reaction as one of the factors.²

Regrettably though, such incidents have become aberrations, as the full enjoyment of freedom of expression online has not lasted long. Over the last decade, the RGC has increasingly developed new legislation and policies in response to the increased prevalence of digital technology. Whilst the development of legislation and policy is critical to adapt to the changing needs of Cambodian society, CCHR is concerned about the contents of some of these developments, and how they may be used to further restrict the right to freedom of expression. They would also be additions to the RGC's legislative toolbox, as several existing laws and provisions of the Criminal Code are already used to restrict this right and unduly and disproportionately penalize those that exercise it to express dissent. As a result, there is increasing self-censorship among the public to express their thoughts on social media. As an example, in 2021, a Battambang farmer who expressed his opinion on social media about a proposal by the former Prime Minister to procure longan fruit from farmers affected by export issues, was arrested and convicted for "incitement".³

¹ Datareportal, Digital 2025: Cambodia (accessed on 23 May 2025), available at: [Digital 2025: Cambodia — DataReportal — Global Digital Insights](#)

² Phnom Penh Post, [PM saves Mt Tamao forest from clearance](#), (7 August 2022).

³ VOA, Battambang Court Fast Tracks Conviction of Longan Farmer, (27 August 2021).

On the other hand, digital platforms have been increasingly exploited by others for personal gain, most notably through online scamming operations in at least 53 scamming compounds across the country. As part of such operations, extensive reporting and investigations have shown that individuals have been trafficked to Cambodia, where upon arrival they have been taken to compounds and forced to engage in online scams, and subjected to psychological and physical abuse if they resist.⁴ Since early 2025, the RGC has made hundreds of arrests as part of a crackdown on scam centers, though reports suggest that victims have been overwhelmingly targeted in arrests, not those behind the operations. Though there is an obvious need to swiftly and comprehensively address this issue, legislation intended to do so must be human rights compliant and not arbitrarily applied. A careful balance between ensuring security and freedom of expression, access to information and privacy must be struck.

It is in this context that CCHR produced this legal analysis. It aims to provide an overview of both existing legislation and draft legislation that relate to the right to freedom of expression, with the purpose of providing a useful tool for civil society, journalists and the public so they can better navigate the current digital space in exercising, claiming and defending their rights and the rights of others. It is also aimed to be useful for policy makers and stakeholders, to highlight concerns regarding current draft legislation and its potential impact on the enjoyment of the right to freedom of expression in the digital age.

⁴ Australian Aid, Human trafficking and forced labour in Cambodia's cyber-scam industry, (29 May 2024).

Part I.

**Overview of
the right to
freedom
of expression**



Freedom of expression is a fundamental freedom that ensures people can discuss, exchange, and debate ideas of all kinds, as well as gain access to information and share it with others, without censorship or reprisals. It is not only a human right in itself, but it also plays a vital basis for the enjoyment of various other rights. Freedom of expression is also a necessary condition for transparency and accountability which are essential conditions for the promotion and protection of human rights, the rule of law, and democracy.⁵

The right to freedom of expression is guaranteed under Article 19 of the International Covenant of Civil and Political Rights (ICCPR), ratified by Cambodia in 1992, and the same article of the Universal Declaration on Human Rights (UDHR). Article 19(2) of the ICCPR states that “everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.”⁶

However, the right to freedom of expression is not an absolute right and may therefore be subject to certain restrictions, outlined by Article 19(3). Accordingly, these restrictions must be:

- provided by law, and
- are necessary for:
 - the respect of the rights or reputations of others;
 - the protection of national security or of public order (ordre public), or of public health or morals.⁷

To assess whether a restriction is justified, a three-part test is used:

(1) Is the restriction provided by the law?

(2) Does the restriction pursue a legitimate aim?

(3) Is it necessary and proportionate?

It is useful to look deeper into each component of the three-part test, in order to apply it practically:

⁵ General Comment No 34 to Article 19 of the CCPR, Human Rights Committee, 102nd session, July 211, page 1.

⁶ ICCPR. Article 19 (Para 2).

⁷ ICCPR. Article 19 (Para 3).

1) Provided by Law

Restrictions must be provided for in law. However, the law must meet the test of “legal certainty”, i.e. it must be formulated in a definite and clear manner, be foreseeable and not have a retroactive effect.⁸ An individual should be able to determine from the content of the law what types of expression are restricted, to allow them to regulate their behavior accordingly. Therefore, laws must not be vaguely worded, which may allow for them to be misused or applied arbitrarily.

2) Pursuing a legitimate aim

Any restriction must pursue one of the legitimate aims mentioned in Article 19(3), subparagraph (a) and (b). Therefore, the only goals that may be legitimately invoked to restrict freedom of expression are: (a) respect of the rights or reputations of others; and (b) the protection of national security or of public order (ordre public), or of public health or morals. Therefore, States cannot prohibit the sharing of information or expressing a view on the basis that they cast a critical view of the government, as such a restriction does not pursue one of the legitimate aims provided for under Article 19(3), (a) or (b).

Regarding Article 19(3)(a), it is also important to recall that all public figures, including those in high political authority, are legitimately subject to criticism and political opposition, by virtue of the position they occupy.⁹ Similarly, a restriction on freedom of expression cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing or to conceal information about the functioning of its public institutions.

In relation to Article 19(3)(b), national security and public order are not synonymous with national, political or government interest.¹⁰ Public order refers to the sum of rules ensuring the peaceful and effective functioning of society, while national security refers to the political independence and/or territorial integrity of the State. The Human Rights Committee has also explicitly stated that the national security clause of Article 19(3)(b) must not be employed to “suppress or withhold from the public information of legitimate public interest” or for the prosecution of journalists, researchers, environmental activists, human rights defenders, or others.¹¹

⁸ Andrew Ashworth and Lucia Zedner, *Preventive Justice* (Oxford University Press 2014), pages 113-114.

⁹ UN Human Rights Committee, General Comment 34, ‘Article 19: Freedoms of opinion and expression’, (12 September 2011), CCPR/C/GC/34, para 38, <https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf>.

¹⁰ UN Human Rights Council, ‘Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies’ (4 February 2016) A/HRC/31/66, para 31, <https://undocs.org/en/A/HRC/31/66>.

¹¹ CCPR/C/GC/34, §30

3) Necessary and proportionate

If freedom of expression is to be restricted, the State must be able to demonstrate in a specific and individualized way that the measure is necessary to target the precise nature of the threat, by establishing a direct and immediate connection between the expression and the threat.¹² The measure must also be proportionate, meaning that the restriction should not go further than is strictly necessary to achieve the legitimate aim. The State should also choose the least intrusive measure to achieve this aim.¹³

The context, form and means of disseminating the expression is also relevant when deciding if a restriction is necessary and proportionate. For example, in the context of political discourse, the value placed upon uninhibited freedom of expression is “particularly high” and therefore closer scrutiny is paid to any measure that limits freedom of expression in relation to public debate regarding figures in the public and political domain.¹⁴ Ideas and opinions which may “offend, shock or disturb”¹⁵ are also protected by freedom of expression, as such are the demands of pluralism and tolerance within a democratic society.¹⁶ Therefore, permissible restrictions on freedom of expression may never be invoked as a justification for suppressing any advocacy of multi-party democracy, democratic tenets and human rights.¹⁷

¹² Ibid., §35

¹³ UN Human Rights Committee, *Vasily Poliakov v. Belarus*, Communication No. 2030/2011, UN Doc CCPR/C/111/D/2030/2011 (17 July 2014), para 8.3, <https://undocs.org/CCPR/C/111/D/2030/2011>.

¹⁴ UN Human Rights Committee, General Comment 34, ‘Article 19: Freedoms of opinion and expression’ (12 September 2011) UN Doc CCPR/C/GC/34, para 38, <https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf>.

¹⁵ European Court of Human Rights, *Handyside v the United Kingdom* App no. 5493/72 (7 December 1976), para 49, <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%5B%22001-57499%22%5D%7D>.

¹⁶ European Court of Human Rights, *Gündüz v Turkey* App no. 35071/97 (4 December 2003), paras 40 and 51, <https://www.legal-tools.org/doc/74a144/pdf/>.

¹⁷ CCPR/C/GC/34, §23



Part II.

**Existing Legal
Framework and
Legislation Impacting
the Enjoyment of the
Right to Freedom of
Expression Online**

The right to freedom of expression is explicitly guaranteed under Article 41 of the Constitution, which states that:

Khmer Citizens shall have freedom of expression of their ideas, freedom of information, freedom of publication and freedom of assembly. No one shall exercise these rights to infringe upon the honor of others, or to affect the good customs of society, public order and national security.¹⁸

Furthermore, Article 31 of the Constitution guarantees respect for Cambodia's international human rights obligations, including those under the ICCPR. It states:

The Kingdom of Cambodia shall recognize and respect human rights as stipulated in the United Nations Charter, the Universal Declaration of Human rights, the covenants and conventions related to human rights, women's and children's rights.

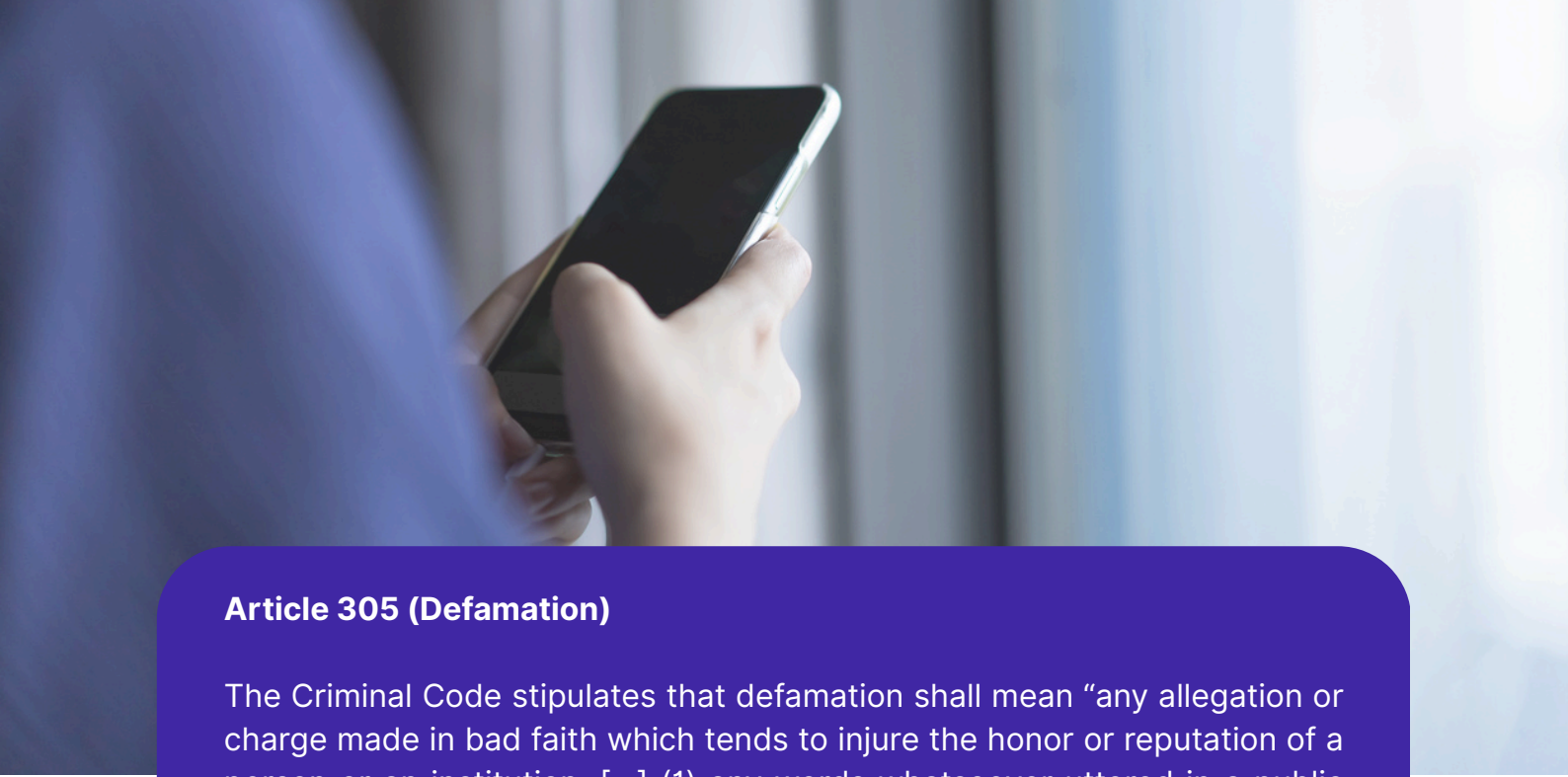
Although the Cambodian constitution purportedly protects the right to freedom of expression through these provisions, on the other hand, a number of provisions of the country's legal framework and legislation are extensively and frequently used to restrict the exercise of the right to freedom of expression, namely the Criminal Code, the Press Law, the Law on telecommunications and the Prakas on social media and Website Control, and the Charter on Professional Journalism:



a. Cambodian Criminal Code

The Cambodian Criminal Code has become the most relied-upon tool to criminalize those who express dissent, particularly members of the political opposition, journalists, human rights defenders and increasingly, social media users. Specifically, these articles are: 305 (Defamation), 494 and 495 (Incitement), 307 (Public Insult), 523 (the questioning of a judicial decision) and 502 (Insult of a Public Official). Not only is their use troubling, but also the fact that the contents of these articles do not reflect the spirit of article 19 of ICCR, therefore making them susceptible to arbitrary application. It is useful to take a closer look at each of these articles to better understand how their formulation and application contribute to the repression of freedom of expression:

¹⁸ Cambodian Constitution. Article 41.



Article 305 (Defamation)

The Criminal Code stipulates that defamation shall mean “any allegation or charge made in bad faith which tends to injure the honor or reputation of a person or an institution. [...] (1) any words whatsoever uttered in a public place or in a public meeting (2) written documents or pictures of any type released or displayed to the public (3) any audio-visual communication intended for the public”.¹⁹ Fines for defamation convictions range between one hundred thousand and ten million Riels, approximately equating to \$25 to \$2,500 USD. In addition, although the charge is not punishable by imprisonment, Cambodians can be imprisoned under article 525 of the Cambodian Criminal Procedure Code 2007 for unpaid fines.²⁰ As asserted by the Human Rights Committee, defamation laws must be crafted in such a way so that they do not stifle freedom of expression and should include a defence of truth and a public interest defence clause – which Article 305 lacks.²¹ The required effect of the actions is also unclear: “injure honor or reputation, social security, affect public order, political stability or good custom of society” is too vague of a formulation, therefore precluding any individual from understanding what type of behavior is criminalized. Further concerning is the inclusion of “institution”, allowing for legitimate criticism or scrutiny of public institutions to potentially be criminalized.

¹⁹ Cambodia Criminal Code. Art 305.

²⁰ Criminal Code Procedure. Article 525.

²¹ CCPR/C/GC/34, §47

Article 494 & 495 (Incitement)

The provisions of the Criminal Code most utilized to restrict freedom of expression are Article 494 and 495, which criminalize “the direct incitement to commit a felony or to disturb social security”, however there is no elaboration or precise definition provided as to what exactly is meant by “incitement” or “social order”. Such vagueness means that the parameters of what is proscribed is unclear, thus allowing for it to be broadly applied as a catch-all charge for dissent and even the exercising of fundamental freedoms more broadly. The lack of precision also means that it fails to meet the test of legal certainty, whereby the law is clearly defined so as to allow individuals to regulate their actions in line with it. Accordingly, the levying of “incitement” against civil society actors in particular has been consistently criticized by human rights experts.²²

The charge is punishable by imprisonment from six months to two years and a fine from one million to four million Riels, where the incitement was ineffective.²³

Article 437-bis (Insulting the King)

In 2018, the Criminal Code was amended to include the offence of lèse-majesté, Article 437-bis, “Insulting the King”. It prohibits “insults addressed to the King” which are defined as “any speeches, gestures, scripts/writings, paintings or items that would affect the dignity of the King”. The charge carries a one to five year prison sentence. This is in contravention of international human rights law, which provides that reputational damage must not be penalized through imprisonment.²⁴ Since the institution of the amendment, CCHR has documented at least 10 cases involving 12 individuals being accused of this offence.²⁵ Notably, at least five individuals were indicted under Article 437-bis on the basis of private conversations – one phone call and one Zoom call.²⁶

²² UN Working Group on Arbitrary Detention, Opinion No. 5/2023 concerning Seng Chan Theary (Cambodia), [A/HRC/WGAD/2023/5](#), §67-71

UN Working Group on Arbitrary Detention, Opinion No. 75/2021 concerning Ros Sakhet (Cambodia), [A/HRC/WGAD/2021/75](#), §64-67

²³ Criminal Code of Cambodia, 495.

²⁴ HRC, CCPR/C/GC/34, §38, 47

²⁵ CCHR, Three years of the Promulgation of Lèse-majesté Law, February 2021

<https://tinyurl.com/CCHR-LM-Snapshot>

CCHR and others, Conviction of Mother Nature Activists is a National Shame, 4 July 2024

<https://tinyurl.com/CCHR-Mother-Nature>

²⁶ Article 19, Blog: How lèse-majesté laws are eroding free speech in Southeast Asia, 19 August 2022

<https://tinyurl.com/Art-19-lese-maj>

Articles 307 (Public Insult), 523 (the questioning of a judicial decision) and 502 (Insult of a Public Official)

Less commonly used but nonetheless troubling are Articles 307, 523 and 502 of the Criminal Code. Those that criminalize “insult”, particularly Article 502, obscure the fact that freedom of expression protects ideas and opinions that may offend, shock or disturb, and that the value placed on uninhibited expression is particularly high when it relates to public figures in the political domain.²⁷ As stated by the Human Rights Committee, “the mere fact that forms of expression are insulting to a public figure is not sufficient to justify the imposition of penalties”.²⁸

Article 425 (False Information)

Article 425 of the Criminal Code proscribes the “communication or disclosure of any false information with a view to inducing a belief that a destruction, defacement or damage dangerous to other persons will be carried out”. The criminalization of spreading misinformation and disinformation is not in accordance with international human rights law, which does not permit generable prohibitions of expressions of an erroneous opinion or an incorrect interpretation of events.²⁹

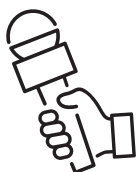
²⁷ ECtHR, *Handyside v the United Kingdom*, App no. 5493/72 (7 December 1976), §49
HRC, CCPR/C/GC/34, §37

²⁸ Ibid, §38

²⁹ HRC, General Comment no.34, §49

Joint Declaration on freedom of expression and “fake news”; disinformation and propaganda. UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, Special Rapporteur on Freedom of Expression of the InterAmerican Commission on Human Rights, and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples’ Rights (2017), §2(a);
Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 23 April 2020, UN Doc. A/HRC/44/49, §49

Significantly however, in August 2024, the Ministry of Justice announced that it was in the process of revising the Cambodian Criminal Code, ostensibly to enhance the country's judiciary, align with international standards and combat transnational crime. According to the Ministry, it was engaging key stakeholders to ensure the reforms align with current and future societal needs and that the reforms are aimed at improving the efficiency, quality and fairness of the judicial system, so that it reflects basic human rights principles. This, therefore, represents a significant opportunity for the abovementioned articles to be revised in accordance with international human rights law.



b. Law on the Press

Several of the provisions of Cambodia's 1995 Law on the Press ("Press Law") are imprecise in their formulation and subsequently create undue restrictions on the media and journalists in carrying out their work without fear of reprisal. Such provisions undermine the potential of well formulated press laws to facilitate genuine press freedom, usually through the inclusion of provisions that prohibit prior censorship, protect the confidentiality of sources, ensure the independence of journalists' associations and allow access for the press to government and judicial processes.³⁰

Regrettably though, this is not the case for the most part of the Law on the Press – particularly those that effectively impose content restrictions:

- Article 11 prohibits the publication of "anything that may affect public order by directly inciting one or more persons to commit violence", punishable by a fine of 1-5 million riels
- Article 12 prohibits the publishing or reproducing of "any information that may affect national security and political stability", punishable by a fine of 1-5 million riels, or the suspension of the publication for maximum 30 days by the Ministry of Information
- Article 13 prohibits the publication or reproduction of "false information that humiliates or contempts [sic] national institutions", punishable by a fine of 2-10 million riels
- Article 14 prohibits the publication of "anything that affects the good customs of society" punishable by a fine of 1-5 million riels

³⁰ Article 19, Memorandum on the Cambodian Law on the Press, (2004) <https://tinyurl.com/4uuc3dcz>

Such prohibitions legitimize the restriction of a wide range of expression that is protected under international law. Furthermore, the use of “may affect” creates a condition whereby there does not necessarily have to be an actual effect, but rather only a *potential* effect. This creates a wide realm of possibility and inevitably makes it more difficult to regulate one’s expression in accordance with the law.

The inclusion of “political stability” in Article 12 is particularly concerning, as it may be used for the purpose of furthering the self-interest of a ruling political party or political figure, thereby undermining the public interest and democratic principles.

The Law also includes inherent contradictions, as Article 1 provides for press freedom, in accordance with the Constitution, and Article 20 states that: “No person shall be arrested or subject to criminal charges as the result of the expression of opinions.” Whilst these are positive provisions of the Press Law, they are undermined by Articles 11, 12, 13 and 14, which significantly limit press freedom and the ability to exercise freedom of opinion.



c. Law on Telecommunications (2015) and the Inter-Ministerial Prakas No. 170 on Social Media and Website Control (2018)

The Law on Telecommunications, which came into force in 2015, created a series of new criminal offences related to the use of telecommunications devices, violations of which are subject to imprisonment and significant fines. These offenses amount to severe restrictions on freedom of expression. On 28 May 2018, the Ministry of Information, Ministry of the Interior (MOI) and Ministry of Posts and Telecommunication issued an inter-ministerial Prakas on website and social media control, supplementing this law and reinforcing its restrictions.

Article 66 of the Law on Telecommunications includes a general prohibition on the “establishment, installation, utilization, and modification of telecommunication infrastructure...which may affect public order and lead to national insecurity are prohibited.”³¹ The punishment for a violation of this offense is a prison sentence of between seven and fifteen years (Article 80).³² Similar to the Law on the Press, the

³¹ Law on Telecommunication. Art 66.

³² Ibid. article 80.

commission of a crime under Article 66 does not require the causation of actual harm, but rather any activity that “may” affect public order or national security is criminalized, rendering the application of this provision extremely broad. While national security and public order are indeed legitimate grounds for restriction of freedom of expression under international human rights law, the criminalization of any form of expression must meet the test of legal certainty. The vagueness of this provision does not appear to meet this test - it is unclear what conduct may affect public order, risking arbitrary application of the clause.

Whilst there are no legislative provisions that explicitly grant the government the power to shut down the Internet, Article 7 provides that: “in the event of force majeure, the Ministry of Posts and Telecommunications or competent ministries or institutions may order relevant telecommunications operators to take necessary measures by relying on the Decision of the Royal Government.”³³ The lack of an explicit explanation as to what “necessary measures” provides for, creates broad discretion as to what measures may be taken, thus not eliminating the possibility of ordering an internet shutdown.

Furthermore, Article 97 provides that “secretly listen[ing] to or record[ing]... dialogue by using personal telecommunication system” is permitted if it is done so “with approval from legitimate authority”, however it does not state what constitutes “legitimate authority”, or that it must be a judicial authority. This therefore leaves open the possibility that surveillance of communications may be sanctioned by a broad range of individuals and without judicial oversight.

The 28 May 2018 Inter-Ministerial Prakas on Websites and Social Media Control (“the Prakas”) aims at “obstructing and preventing all publications or news content sharing or written messages, audios, photos, videos, and/or other means intended to create turmoil leading to the undermining of national defense, national security, relation with other countries, national economy, public order, discrimination and national culture and tradition.”³⁴ It covers “all news contents or written messages, audios, photos, videos, and/or others means”³⁵ in “website publications” as well as “any kind of social media network” on the internet in Cambodia,³⁶ and applies to all websites and social media networks in Cambodia.³⁷

The Prakas establishes a joint “specialized unit” including representatives of the Ministry of Information, MOI and Ministry of Posts and Telecommunications, whose task it is to “cooperatively monitor, study, research, find out illegal business

³³ Ibid. article 7.

³⁴ Social Media Prakas, clause 2.

³⁵ Social Media Prakas, clause 1.

³⁶ Social Media Prakas, clause 2.

³⁷ Social Media Prakas, clause 3.

activities and publications on websites and social media” and to take action against them.³⁸ According to the MOI, the Unit was created to combat cybercrime, and enforce the new offense of lèse majesté.³⁹ Together the task force has the power to surveil, share information, sanction, block or shut down Internet Service Providers (“ISPs”) and take legal action against those individuals in violation of the Prakas.

The Prakas creates a number of offences, including:

- Clause 8(a): Creating social turmoil;
- Clause 6(c): Publicizing information willing to create turmoil;
- Clause 6(c), Clause 8(a): Undermining national Defense;
- Clause 6(c), Clause 8(a): Undermining national security;
- Clause 6(c), Clause 8(a): Undermining relations with other countries;
- Clause 6(c), Clause 8(a): Undermining public order;
- Clause 6(c): Undermining national economy;
- Clause 6(c), Clause 8(a): Creating discrimination;
- Clause 6(c), Clause 8(a): Undermining national culture and tradition;
- Clause 7(c): Publicizing illegal contents which are considered as incitement, breaking solidarity, discrimination, create turmoil by will, leading to the undermining of national security, and public interests and social order;
- Clause 6(c), Clause 7(c), Clause 8(a): Publicizing/operating “illegally” (Clause 6 (c), 7 (c), 8 (a));
- Running illegal business activities;
- Clause 8(c): Publicizing news or written messages, audios, photos, videos, and/or other means which considered as contrary to the law of the Kingdom of Cambodia.

In addition to these provisions, the Prakas orders, inter alia, all ISPs to “install software programs and equip internet surveillance tools to easily filter and block any social media accounts or pages” deemed “illegal”, and the Ministry of Posts and Telecommunications to “block or close” websites and social media pages containing content “considered as incitement, breaking solidarity, discrimination and willfully creating turmoil leading to undermining national security, public interest and social order.”

Such actions constitute an unjustified and disproportionate violation of freedom of expression. Although these restrictions are contained in a legal instrument, they are

³⁸ Social Media Prakas, clause 4

³⁹ Kann Vicheika, ‘Cambodia Forms Task Force to Monitor ‘Fake News’ on Social Media’, Voice of America (6 Jun 2018) <https://www.voacambodia.com/a/cambodia-forms-task-force-to-monitor-fake-news-on-social-media/4425534.html>.

so broad and imprecise that they do not enable individuals to regulate their conduct accordingly, and therefore cannot be said to be provided by law. In particular, terms such as “offensive content”, “willing to create turmoil”, or “illegal business activities” are excessively vague and broad.

Clause 2 of the Prakas sets out eight goals underpinning its adoption, namely the protection of “national defense”, “national security”, “relation with other countries”, “national economy”, “public order”, “discrimination”, “national culture”, and “tradition.”

“National economy” does not constitute a legitimate aim. The terms of “national culture” and “tradition” are overly broad and thus vulnerable to appropriation - they would only be considered legitimate aims if they fell into the ambit of “public morals.”

Where national security is relied on as a legitimate ground for restriction of the right to freedom of expression, a direct and immediate connection between the expression and the purported threat must be established.⁴⁰ It must be shown that (a) the expression is intended to incite imminent violence; (b) is it likely to incite violence and (c) there is a direct and immediate connection between the expression and the likelihood of such violence.⁴¹ Using ‘national security’ as a ground to restrict speech should be limited to “situations in which the interest of the whole nation is at stake, which would thereby exclude restrictions in the sole interest of a Government, regime or power group... Similarly, public order (ordre public) must be limited to specific situations in which a limitation [to speech] would be demonstrably warranted.”⁴²

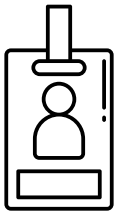
The actions that justify the restriction of freedom of expression are not defined in the Prakas. Instead, the language used throughout is overly broad and unduly vague: terms such as “fake news”, “illegal broadcasts”, “social turmoil”, “relations with other countries”, “illegal contents”, and “illegal activities” lack definition to constitute a reasonable and proportionate restriction to freedom of expression.

Further, the far-reaching effects of the Prakas, namely the disappearance of online privacy, suspension of websites, shutting down of social media accounts, and the fact that there is no mention of judicial supervision or of any possible recourse to those wanting to challenge the actions taken by the Specialized Unit, mean that the reach of the Prakas is widely disproportionate to its stated aims and as such, contravenes human rights law.

⁴⁰ UN Human Rights Committee, ‘General Comment No. 34: Article 19: Freedoms of opinion and expression’ UN Doc CCPR/C/GC/34 (12 September 2011), para 35.

⁴¹ UN Human Rights Council, ‘Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’ UN Doc A/HRC/17/27 (16 May 2011), para 73.

⁴² UN Human Rights Council, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’, UN Doc A/71/373 (6 September 2016), para 18.



d. Charter for Professional Journalism & Journalist ID Cards

Introduced under the pretense of supporting the media, the Charter for Professional Journalism was promulgated by the Ministry of Information in August 2024.⁴³

In a consultation workshop convened by the Ministry with media associations and journalists, the Minister stressed that such an instrument was necessary to address the spread of fake news, and that a “lack of clear sources” and “stakeholders’ explanations” in news articles had jeopardized public trust.⁴⁴ Stakeholders were provided only nine days to provide inputs to the draft, with the Charter being adopted just four days later, precluding further stakeholder deliberation on how the inputs would be reflected.⁴⁵

As CCHR has previously expressed concern about, the scope of the Charter and related enforcement mechanisms are ambiguous, raising concerns that it would be arbitrarily and selectively applied. Further concerning is the lack of a public interest override, proactive measures for verifying information prior to publication and notably, its potential use to silence critical opinions or reporting that is viewed as unfavorable to influential figures. Its prohibition of the dissemination of content that “affects the culture, traditions and good customs of the nation” runs risk of being broadly interpreted to censor online content that is critical of the Government.⁴⁶ A number of UN Special Rapporteurs on the Government to suspend the Charter and thoroughly review and reform it, and to protect and promote independent, free and plurality media as a vital pillar of democracy.⁴⁷

The introduction of the Charter occurred around the same time as the Ministry of Information announced that press cards would now be digitized.⁴⁸ The cards were ostensibly introduced to ensure authenticity and prevent forgery of press cards, and with the aim of maintaining a clear record of journalists in the country.⁴⁹ State registration or licensing systems for journalists, according to the Human Rights Committee, are incompatible with Article 19(3). Limited accreditation schemes are permissible only for the purpose of providing journalists with privileged access to places and or events.

⁴³ CCHR, <https://tinyurl.com/CCHR-Journalism-Charter>

⁴⁴ CCHR, ‘State of Freedom of Expression, press freedom and access to information’, (2024) p.7-8

⁴⁵ CCHR, ‘State of Freedom of Expression, press freedom and access to information’, (2024) p.7-8

⁴⁶ Ibid.

⁴⁷ OHCHR, ‘Cambodia: UN experts call for suspension of professional journalism charter’, 12 September 2024 <https://tinyurl.com/ys3726mp>

⁴⁸ Khmer Times, Ministry launches MoINFO App for journalist ID cards (03 March 2025).

⁴⁹ CCHR, ‘State of Freedom of Expression, press freedom and access to information’, (2024) p.15



e. Sub-decree on the National Internet Gateway (NIG)

The Sub-decree on the Establishment of the National Internet Gateway (NIG), drafted by the Ministry of Post and Telecommunications in July 2020, mandates that all internet traffic circulating within and coming into Cambodia be channeled through a single gateway. The stated aims of the NIG, according to Article 1 of the Sub-decree, are to facilitate and manage internet connections to strengthen revenue collection, protect national security and “preserve social order, culture and national tradition”.

As CCHR, numerous other Cambodian civil society organizations and UN Special Rapporteurs have stressed however, the NIG Sub-decree provides the RGC with the means to monitor and surveil internet activity, intercept and censor digital communications, and enables the collection, retention and sharing of personal data.⁵⁰ Such extensive powers not only fundamentally undermine the right to freedom of expression and access to information, but also the right to privacy.

Article 6 provides that government-appointed NIG operators can block or disconnect any online connections or content that are deemed to “affect safety, national revenue, social order, dignity, culture, traditions and customs”. The formulation of this article is overly broad and therefore may enable the authorities to conduct mass surveillance of private communications online, without providing grounds for doing so, and also extensive censorship of online content, given the vagueness of the conditions. It would therefore not adhere to the permissible restrictions on exercising the right to freedom of expression under Article 19(3), specifically regarding the need for legal clarity.⁵¹ Furthermore, “national revenue” is not a legitimate purpose for which exercising the right to freedom of expression may be restricted.

Article 14 provides that NIG operators can “prepare and maintain technical records and lists of allocated IP Address and identification of route traffic through NIG, compile and maintain reports and relevant documents concerning the connections and all internet traffic”, without stating the need for a cause or purpose for doing

⁵⁰ CCHR, ‘Sixth Annual Report of the Cambodia Fundamental Freedoms Monitor’, (2022), <https://tinyurl.com/FFMP-22>, p.7-10
CCHR & others, ‘Joint statement – CSOs call on the Royal Government of Cambodia to repeal the sub-decree on the establishment of the National Internet Gateway’, 19 February 2021, <https://tinyurl.com/NIG-Statement>

CCHR, ‘State of Freedom of Expression, press freedom and access to information’, (2024) p.7

⁵¹ HRC, CCPR/C/GC/34, §24-25

so. This thereby allows for the building of profiles for certain users or organizations without a stated purpose, raising concern that individuals or organizations who are deemed critical of the authorities may be subjected to such surveillance. It would therefore not meet the necessity and proportionality test for permissible restrictions on freedom of expression under international human rights law.⁵² The same article also allows such operators to retain traffic data for a year and provide other network information as requested by authorities.

Furthermore, Article 16 provides for overbroad penalties for non-compliant telecommunications operators, which would not meet the proportionality requirement under international human rights law.

Although the Sub-decree was signed by the Prime Minister in February 2021, and the NIG was due to be enforced from 16 February 2022, its planned implementation has been delayed by the RGC to an unspecified date. The cited reasons for the delay have differed, with some government spokespeople citing COVID-19, and others citing infrastructure challenges.⁵³ In October 2025, however, the media reported that a document from the Ministry of Planning titled “Install and Manage National Internet Gateways”, dated May of the same year, included details about the RGC’s plans to start work on the NIG infrastructure in 2026.⁵⁴ According to the media reporting on the document, it states that “Through the use of big data, artificial intelligence technology, the Royal Government can analyze and manage social media broadcasts”.⁵⁵ At the time of publishing this Legal Analysis however, this information has not been publicly announced by the RGC. If the stated plans are true, it represents a concerning development in the implementation of the NIG.

⁵² Ibid, §22

⁵³ Civil Rights Defenders, Cambodia Should Scrap Rights-Abusing National Internet Gateway, 16 May 2022, <https://tinyurl.com/CRD-statement-NIG>

⁵⁴ Nikkei Asia, Cambodia resurrects plan for controversial internet gateway, 20 October 20225 <https://tinyurl.com/Nikkei-Asia-NIG>

⁵⁵ Ibid.

Part III.

Draft legislation and policies Impacting Enjoyment of the Right to Freedom of Expression, Access to Information and Privacy Online



Having now outlined the existing legal and policy provisions that restrict the exercising of the right to freedom of expression in Cambodia, it is worth looking at how current draft legislation risks further restricting the enjoyment of this right.



a. Draft Cybercrime Law

Since 2010, the drafting process of a Cybercrime Law has been underway, with at least three versions being produced since then. In 2025, the latest draft of the law was produced. As with previous drafts, several concerning provisions remain in place, and would have a detrimental impact on the right to freedom of expression, if the draft is adopted in this current form.

According to Article 1 of the draft, the purpose of the Cybercrime Law is to ensure the integrity of the use and management of computer systems and computer data, protect security and public order, and protect the rights of individuals by setting out measures to deter, prevent and suppress cybercrime. Many of its provisions however criminalize the exercise of the right to freedom of expression with disproportionate penalties, with the articles using broad terms and lacking imprecision.

Article 42 on ‘Information technology-related abuse’ states that an individual who “intentionally causes intimidation, threat or abuse to another person by information-technology related means could face imprisonment ranging from one month to two years, and a fine from 2 – 10 million Riels. “Intimidation, threat or abuse” are not defined, and are notably subjective due to the use of “causes”, meaning the focus is placed on the perceived impact rather than the action committed by the individual. Such vagueness does not therefore meet the test of legal certainty, to allow for individuals to regulate their actions in accordance with the law.

Article 43 on ‘Defamation’, which stipulates that the “exaggerated claim or insincere blame for any act that harms the honor or reputation of an individual or institution through information technology”, is particularly concerning. That rhetoric or expression is exaggerated, whether through emotional or expressive language or phrases, is not a permissible ground for restriction. Prohibiting exaggeration seriously undermines the right to express oneself and one’s opinion, and strips expression of its emotion. Exaggeration can be cited as a defense against

defamation under the doctrine of rhetorical hyperbole, whereby the statement is an obvious exaggeration not meant to be taken as fact.⁵⁶ Such hyperbolic statements are therefore not considered as statements of fact, which is crucial for defamation cases, where proving a claim is true or false is a necessary element. The use of the phrase “insincere blame” is also troubling, as the sincerity or insincerity of a statement is not a factor in proving or disproving defamation claims – rather, the factual truthfulness of a statement is the critical element. Furthermore, that a defamation claim can be made against an institution contravenes international human rights law and standards, which stipulates that States should not prohibit criticism of institutions.⁵⁷ It also holds that “imprisonment is never an appropriate penalty” for defamation.⁵⁸ However, Article 43 stipulates that in cases where this act causes “serious harm”, the offender may face between one to six months imprisonment, and fines for this charge range from two million to 20 million Riels. The inclusion of imprisonment as a punishment is also not consistent with Article 305 of the Criminal Code, whereby defamation is punishment by fine only. It may therefore be deduced that Article 43 is aimed at increasing the potential penalty for defamation, which in Cambodia is already inordinately used to penalize legitimate exercise of the right to freedom of expression, This is particularly concerning, given that presently, a significant proportion of defamation cases – if not the majority - are brought against.

In addition, Article 44 of the draft states that “the use of any insulting, derogatory or rude language without imposing blame on any act through information technology” shall be fined and in cases where the act “causes serious harm to the victim”, punished by imprisonment from one to six months. Therefore, as with Article 44, this article is also not consistent with corresponding Article 307 of the Criminal Code of Cambodia (public insult) for which there is only a fine for the offender. The Human Rights Committee has asserted that Article 19(2) “embraces even expression that may be regarded as deeply offensive”.⁵⁹ Whilst it continues that such expression may be restricted, it may only be done so in accordance with 19(3). By this measure, language that is “insulting”, “derogatory” and “rude” would be protected.

The inclusion of imprisonment as a penalty for Articles 43 and 44 is a particularly concerning development, as it constitutes a departure from their corresponding articles in the Criminal Code (305 and 307) and increases the severity of penalties for these charges. This would therefore suggest that somehow, expression through

⁵⁶ Article 19, Defining Defamation – Principles on Freedom of Expression and Protection of Reputation, p.12-13, <https://tinyurl.com/Article-19-Defamation>

⁵⁷ HRC, General Comment No.34, §38

⁵⁸ Ibid, §47

⁵⁹ Ibid, §11

information technology that is deemed to fall under the provisions of Articles 43 and 44 warrants a heightened penalty by virtue of the fact that it is expressed through information technology. The rationale behind this remains unclear, thus giving rise to skepticism about the intention behind the heightened penalties included in these articles, and concern regarding their potentially arbitrary application.

Article 49 of the current draft states that “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” shall be subjected to three to five years’ imprisonment. The criminalization of spreading misinformation and disinformation, as this article appears to do, is incompatible with human rights law.⁶⁰ International law, as asserted by the Human Rights Committee, does not permit generable prohibitions of expressions of an erroneous opinion or an incorrect interpretation of events.⁶¹

In addition to the potential implications of these concerning provisions on the right to freedom of expression, the current draft of the Cybercrime Law also contains provisions which may infringe on the right to privacy. This right is guaranteed under Articles 12 and 17 of the UDHR and ICCPR, respectively, which state that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.⁶²

Article 5 of current draft law on cybercrime provides broad power to the judicial police in charge of anti-cybercrime to investigate the offence without providing notification to the court.⁶³ In addition, Article 12(1) of the draft stipulates that “at the request of the competent authority for the collection of the evidence, if there are reasonable grounds that evidence of a crime exists on a service provider’s computer system or otherwise under the control of the service provider, the service provider shall preserve any and all relevant computer data traffic data or subscriber information”.⁶⁴ These articles provide wide ranging power to the judicial police in charge of anti-cybercrime to investigate and preserve the data without notification to the court or guidance from the court. Such articles may therefore infringe on an individual’s right to privacy.

⁶⁰ Joint Declaration on freedom of expression and “fake news”, disinformation and propaganda. UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, Special Rapporteur on Freedom of Expression of the InterAmerican Commission on Human Rights, and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples’ Rights (2017), §2(a); Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 23 April 2020, UN Doc. A/HRC/44/49, §49

⁶¹ HRC, General Comment no.34, §49

⁶² UDHR. Art 12.

⁶³ Draft law on Cybercrime. Art 5.

⁶⁴ Draft law on Cybercrime. Art 12.

Furthermore, Article 7 grants power to the competent ministries or institutions which granted the business permit may suspend or revoke that business permit.⁶⁵ Also the article 18 stated that any person who is dissatisfied with the suspension or the revocation of the business permit, certificate or license as stated in the article 7 of this law is entitled to file a complaint to the competent minister or head of relevant institution within 30 days of being noticed of such a decision.⁶⁶



b. Draft Law on Access to Information

For approximately two decades, a law on access to information has been in the drafting process, but is yet to be finalized. The process to date has been transparent and consultative, enabling valuable dialogue with experts and stakeholders, and has facilitated public participation through an online portal. A Technical Working Group on the Drafting of the Access to Information Law was set up to facilitate engagement with experts and stakeholders, consisting of government representatives, United Nations representatives and civil society representatives. This should be the standard by which all new laws in Cambodia are drafted and consulted. A website was also created to display drafts of the law and provide the opportunity for comments from the public - though it has not been updated.⁶⁷

Access to information is now recognized as a universal human right. The right is derived from the right to freedom of expression which includes not only the right to “impart” information and ideas, but crucially also the rights to “seek” and “receive” them. Access to information does not only benefit individuals but also the public at large, to promote press freedom, freedom of expression and democracy. Some of the benefits of access to information include but are not limited to: participatory democracy, fighting corruption and government wrongdoing, ensuring accountability for decision- and policy-makers, economic and sustainable development, the facilitation of informed decision-making and the promotion of respect for human rights.

⁶⁵ Draft law on Cybercrime. Art 7.

⁶⁶ Draft law on Cybercrime. Art 18.

⁶⁷ CCHR infographic on access to information in Cambodia, available at:
<https://cchrcambodia.org/en/publications/infographics/access-to-information-in-cambodia-148>

Despite the encouraging process to draft the law, there are several provisions of the current draft that are inconsistent with international human rights law and standards.

Article 4 of the draft lists the relevant technical terms, including “official documents”, a vague and subjective term and does not provide specification, which may therefore restrict the extent of access granted.

Article 20 of the draft outlines the confidential information which cannot be disclosed to the public. However, it fails to prescribe a consideration of whether substantial harm would be inflicted by releasing such information. Further, Article 20(7), which exempts “other confidential information as stipulated in the prohibited provisions” from disclosure, could be used as a catch-all clause to justify the withholding of access to information in the public interest but that the Government or its members may deem detrimental to their public reputation.⁶⁸

To meet international standards, exemptions must be explicit, unambiguous and with a narrow scope. International human rights standards stipulate that non-disclosure of information must be justified on a case-by-case basis and that exemptions may only apply where “there is a risk of substantial harm to the protected interest and where that harm is greater than the overall public interest in having access to the information”.⁶⁹

By this measure, Article 20.7 is overly broad, lacks specificity and may therefore be considered a blanket provision. In addition, the article contains no “three-part test” to determine whether exempted information can be withheld from the public. International standards of access to information require application of the three-part cumulative test relating to freedom of expression: is the exemption provided by law - adhering to the principles of legal certainty; does the exemption pursue one of the legitimate purposes set out in Article 19(3); and in accordance with the principles of necessity and proportionality, is the exemption necessary and the least restrictive means required to achieve the purported aim.⁷⁰

Article 26 of the draft does not provide protection for whistleblowers, which should be added to this article, if the disclosure is in the public interest. Further, article 33 of the draft law imposes the disproportionate criminal sanction of imprisonment.

⁶⁸ Draft law of access to information. article 20.

⁶⁹ UNGA, Report of the UN Special Rapporteur on the right to freedom of opinion and expression, A/68/362, §76 <https://tinyurl.com/UNSR-FreedEx-2013-A21>

⁷⁰ HRC, General Comment no. 34, §22
UNGA, A/68/362, §76



c. Draft Law on Cybersecurity

In November 2022, Cambodia's Ministry of Post and Telecommunications (MPTC) announced that it had drafted a law on cybersecurity, which has the stated aim of determining "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."⁷¹ Since then, the Ministry has been reviewing and revising the draft in accordance with inputs from stakeholders. However, the current draft of the law is likely to have a detrimental impact on the rights to privacy and freedom of expression and access to information.

Article 4 of the draft provides wide-ranging power to the Digital Security Committee (DSC), an executive body, coordinated by the MPTC, which is tasked with ensuring "efficiency and effectiveness in fulfilling the role of leading, coordinating, and promoting the governance of digital security".⁷² Some of the most concerning powers granted to the DSC include 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 incident⁷³; "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"⁷⁴; 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.⁷⁵ These significant powers vested in the DSC are overbroad and do not comply with the principles of legality and proportionality of article 19 ICCPR. In accordance with articles 19 and 21 of the draft, the DSC is not required to obtain prior approval from a judicial authority or oversight body before issuing any orders to "provide information and allow the use of related electronic devices" or allow access to "any relevant computer or computer system". This is in contravention of the principle of legality, which requires that any measure that may interfere with an individual's rights to privacy and freedom of expression must be applied with strong judicial safeguards.

⁷¹ Draft law on Cybersecurity. art 1.

⁷² Draft law on Cybersecurity. art 4.

⁷³ Draft law on Cybersecurity. art 19.

⁷⁴ Draft law on Cybersecurity. art 21.

⁷⁵ Draft law on Cybersecurity. art 19.

Access Now & International Commission of Jurists (ICJ), Legal Analysis: Cambodia Draft Law On Cybersecurity <https://tinyurl.com/2s3netfs>

Article 21(1) of the draft, which authorizes the DSC to access "any relevant computer or computer system", may be detrimental to the right to privacy, as it does not specify that it would seek to target data necessary to prevent a "cybersecurity threat". It also does not appear to be the least intrusive measure available for that limited aim, in accordance with international human rights law.⁷⁶ This broad formulation may allow the DSC to access private data held on a computer system well beyond what is required for the situation in question. The lack of provisions in the draft to establish an oversight mechanism for the DSC compounds this concern of overbroad access to private data being granted to the DSC.

Article 24 establishes Cybersecurity Inspectors, who are appointed as "judicial police officers" by the Minister of the MPTC in order to "monitor, study, inspect, and strengthen the enforcement of this law". Such inspectors are provided with overbroad powers, which run the risk of interfering with the rights to privacy, freedom of expression and information. Such powers include the ability 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). It does not enunciate the specific measures they are authorized to take to carry out these functions, thus leaving a broad realm of potential measures.



d. Draft Law on Personal Data Protection

On 19 February 2021, the Ministry of Post and Telecommunications (MPTC) announced that it would begin the process of drafting a personal data protection law. The MPTC then made the Draft Law on Personal Data Protection available to a select number of private organizations and companies in September 2023, to receive their input on the draft – no version has yet been released to the public. The instigation of this process occurred against a broader backdrop of countries around the world revising or drafting anew respective data protection laws, in recognition of the fact that in an increasingly digitized world, more and more data is being collected, shared and stored than ever before, bringing with it related

⁷⁶ HRC, CCPR/C/GC/34, §34

a privacy concerns. In June 2025, the MPTC issued a revised Draft Law on Personal Data Protection (“Draft Law on PDP”). Its stated intent is to regulate the processing (including the collection, use and disclosure) of personal data and to protect the right to privacy of natural persons in Cambodia.

The right to privacy is guaranteed under Article 40 of the Constitution of the Kingdom of Cambodia. It is also protected under the Civil Code, the Criminal Code and the Code of Criminal Procedure. In international human rights law, the right to privacy is guaranteed by Article 17 of the ICCPR, ratified by Cambodia in 1992. Article 17 provides that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence”, and that “everyone has the right to the protection of the law against such interference”.

Restrictions on enjoyment of the right to privacy must meet the legality, legitimacy, and necessity standards, meaning that the government’s ability to interfere with an individual’s privacy rights must be clearly provided for in law, in pursuit of a valid purpose, and both proportional in scope and directly related to that valid purpose.⁷⁷ Government surveillance that is broad, indefinite, or secretive is therefore a violation of international human rights law. The Human Rights Committee has stipulated that Article 17 requires States to put in place a legal framework that prohibits violations of privacy by private individuals and entities, as well as the protection of the right.

It further stipulates that every individual has the right to know “what personal data is stored in automatic data files, and for what purposes”, “be able to ascertain which public authorities or private individuals or bodies control or may control their files” and “the right to request rectification or elimination”.

These principles outlined by the Human Rights Committee – the right to be informed, the right of access, the right to rectification, and the right to erasure (or “the right to be forgotten”) – form the basis for many data protection laws. The European Union’s General Data Protection Regulation (GDPR) is one such example, and has been the blueprint for many other data protection laws around the world, such as those of Brazil and the UK.

Whilst data protection legislation primarily engages the right to privacy, it also impacts on the right to freedom of expression, particularly when that right is exercised online or in digital format, as it can have a deterrent or censoring effect on individuals. As asserted by the Human Rights Committee, individuals who have

⁷⁷ ICCPR, Article 19

reason to fear that their communications may be subjected to monitoring by the government, will therefore be less likely to express themselves for fear of the consequences.⁷⁸

CCHR has assessed some positive provisions of the Draft Law on PDP, such as the provision that allows not-for-profit bodies to process sensitive personal data of a data subject when doing so as part of the normal course of business and with safeguards, Article 14(d); and the removal of the requirement that data controllers store all collected personal data in Cambodia, Article 23, in line with international best practice. Whilst it welcomes these provisions, CCHR's analysis has also revealed some troubling aspects of the current draft. Namely, the draft's lack of precision regarding exceptions to data processing requirements, the processing of data without consent of the individual, and the lack of an independent data protection authority. These issues can be predominantly found across articles 7, 14 and 4 of the current draft.

Article 7

Article 7 of the Draft PDP covers the Legal Basis for Processing Personal Data. It states that the processing of personal data should be based on one of the following legal bases:

- a. Consent of the data subject;
- b. The necessity of performing a contract to which the data subject is a party, or at the request of a data subject prior to entering into a contract;
- c. The necessity of the data controller to perform legal obligations as required by law;
- d. The necessity for the protection of the vital interests of the data subject or another natural person;
- e. The necessity for the purposes of the performance of a task carried out in the public interest;
- f. The necessity for the purposes of legitimate interests pursued by the data controller or a third party

The articles of particular concern are 7(d), 7(e) and 7(f), due to the fact that these exceptions are quite broadly worded and therefore leave room for arbitrary application. According to these articles, an individual's data may be processed without their consent, as the terms "public interest", "legitimate interests" or the "vital interests of... another natural person" are not enunciated. Whilst an exhaustive list or definition of all scenarios that may require exemption, best practice on this

⁷⁸ HRC, CCPR/C/GC/34, §3 - 4

issue is evident in the EU and UK GDPR, as they provide examples of “legitimate interests” (marketing, fraud prevention, IT security, indicating possible criminal acts or threats to public security, ensuring network and information security) and narrowly drawn “public interest conditions” (the UK GDPR sets out a list of 23 “narrowly drawn” examples).⁷⁹

These broad exemptions under Article 7(d), (e) and (f) therefore do not meet the legality requirement under international human rights law as they are not formulated in a sufficiently precise way, therefore granting a data controller broad discretion of their application.

Article 14

Article 14 of the Draft PDP covers the Protection of Sensitive Personal Data. It prohibits the processing of “sensitive personal data” (medical data, financial data, children’s data or personal identifiers – passport or national identification cards). However, it provides nine scenarios in which exceptions can be made to the prohibition, in addition to one of the legal bases under Article 7.

Similar to Article 7(d), Article 14(c) references “vital interests” as a potential exemption, but does not explicitly mention what these may be. This is also the case for Article 14(g), which also includes mention of “public interest”, without explicit detail as to what this may entail.

Article 14(e) is also concerning regarding the processing of data without consent, as it provides that sensitive data may be processed when the data has “manifestly been made public by the data subject”. This exemption requires narrow interpretation for application, particularly with regard to personal data that is available through social media. As summarized by the International Center for Not-for-Profit Law (ICNL) in its analysis of the Draft PDP, “Social media users that post about their political opinions, beliefs, or other sensitive information with the intent of sharing with their friends and family may not be aware that their information is public and accessible to third parties to be processed in ways that they did not intend. Processing that data would be incompatible with the object and purpose of the data protection law”.⁸⁰

⁷⁹ ICO, ‘What are the substantial public interest conditions?’

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-substantial-public-interest-conditions/> <https://tinyurl.com/379r5sd5>

⁸⁰ ICNL, Cambodia’s Draft Law on Personal Data Protection,

https://data.opendevdevelopmentcambodia.net/en/dataset/087a5b1e-bc04-4da1-8870-c375b87e01f2/resource/fd8b0cb3-afc4-44d0-a9c8-1e482a9f7e2c/download/icnl-comments-on-cambodia-draft-law-on-personal-data-protection_july2025.pdf

CCHR would therefore recommend that this article be revised to clarify that manifestly publicly available data does not include data that has been published on social media and means only data that the data subject has deliberately made publicly available.

Article 4

Article 4 of the Draft PDP provides for the Ministry of Post and Telecommunications to act as the office that will oversee the implementation of the law and its provisions. It is international best practice that the body that oversees data protection is sufficiently independent and autonomous. This includes provisions such as a fixed term for data commissioners, removal of commissioners for cause only and a dedicated budget which it has full control over. A lack of independence in any data commission or oversight body runs the risk that the issue of data protection and or the oversight body will be politically weaponized. This concern is particularly pronounced, given the existing concerns regarding the lack of precision in some of the formulations in other articles of the Draft PDP, as mentioned above.

Conclusion

This legal analysis has aimed to demonstrate how existing legal provisions have created an environment in which exercising the right to freedom of expression online is already subject to significant restrictions, and that a number of pieces of draft legislation risk restricting this right even further. In the most concerning examples, such as the Draft Law on Cybercrime, the crime of “defamation” has not only been ascribed disproportionate penalties, but such penalties represent an increase in severity in comparison to the equivalent in existing legislation. This is particular cause for concern, given that the crime of “defamation” (Article 305 of the Criminal Code) is often arbitrarily brought against civil society actors – human rights defenders, journalists, political activists and even social media users – for expressing personal views about the actions of figures in political leadership or influential businesspeople.

As this legal analysis has shown, the common denominator across these draft laws is the lack of precision in the formulation of their provisions, giving rise to concern that they may be applied in a way that is inconsistent with their stated purpose. CCHR calls on the Royal Government of Cambodia (RGC) to meaningfully consult academics and human rights organizations with expertise on the right to freedom of expression, access to information and data protection to ensure precise wording in these draft laws, to allow Cambodians to understand and act in accordance with the law. Engagement must go further than consultation though, and inputs must be meaningfully integrated in good faith.

The draft laws outlined in this analysis, in their current form, require significant revision to ensure they comply with Cambodia’s obligations under international human rights law. CCHR therefore calls on the Royal Government of Cambodia (RGC) to constructively engage with individuals and organizations to ensure this compliance, and amend the current drafts in the interests of all Cambodians and respect for their right to freedom of expression.

Recommendations to the Royal Government of Cambodia (RGC):

- The Ministry of Justice (“MoJ”) may consider amending, replacing, or revising Articles 305, 494, 495, 437-bis, 307, 523, 502 and 425 of the Criminal Code, as part of the current process to revise the Code, to ensure the right to freedom of expression is adequately protected by and provided for in legislation.
- Consider the amendment of Articles 11, 12, 13, and 14 of the Law on the Press (1995), to ensure that content restrictions do not unduly restrict the right to freedom of expression.
- Regarding the Law on Telecommunications (2015) and the Inter-Ministerial Prakas No. 170 on Social Media and Website Control (2018):
 - Consider revising Articles 66 and 7 of the Law of Telecommunications to ensure greater precision and clarity in their formulation, including specific examples, and therefore legal clarity in line with the legality principle in the three-part test in international law
 - Consider revising Clauses 2, 6, 7 and 8 of the Inter-Ministerial Prakas to ensure they are sufficiently precise and clear in their formulation, therefore allowing individuals to act accordingly
- Consider significant revision or revocation of the Charter on Professional Journalism, to ensure it facilitates rather than restricts media freedom.
- Consider the extensive revision or revocation of the Sub-Decree on the National Internet Gateway (NIG), given the significant power it provides for the monitoring, surveillance, interception, and censoring of online activity, which may constitute government-overreach.
- Consider the revision of Articles 5, 7, 42, 43, 44, and 49 of the Draft Law on Cybercrime, specifically the removal of imprisonment as a penalty under Articles 42 and 43, to ensure the legislation is in line with the Criminal Code of Cambodia.
- Consider the revision of Articles 4, 20, 26, and 33 of the Draft Law on Access to Information, to ensure it allows for the meaningful enjoyment of the right to access to information, without undue and overly broad restrictions.

Recommendations to the Royal Government of Cambodia (RGC):

- Consider the revision of Articles 4, 21, 24, 26, and 27 to ensure that the authority granted to the Digital Security Committee (DSC) is proportionate to the stated aim of the legislation and compliant with international human rights law, and the need for any restrictions on freedom of expression being the “least intrusive measure”.
- Consider the revision of Articles 4, 7, and 14 of the Draft Law on the Personal Data Protection (PDP), to ensure it is aligned with international best practice regarding data protection legislation.



ប្រជុំបណ្តាញសិទ្ធិមនុស្សកម្ពុជា
Cambodian Center for Human Rights