
KONRAD
ADENAUER
STIFTUNG
1. Data Protection Law
2. IP Law & Digitalisation
3. Digital Markets Law
4. Cybercrime Law
5. Law & A.I
Smart Regulation Drives
Smarter Innovation
01
02
03
04
LAW BRIEF 2025:
BITS, BYTES & BILLS

## ABOUT LAW BRIEF

It is a compilation of legal articles produced by KAS For Legal Youth (KASFLY) fellows in the program. As a key learning output, KASFLY fellows are required to author a law brief article. These articles focus on issues of interest of the fellows on debating recent trends, challenges, and issues in both the international and national legal arena that may provoke key development and threaten the justice system at large.

Initiated by Konrad-Adenauer-Stiftung (KAS) Cambodia and the Royal University of Law and Economics, the Law Brief publication aims to provide comprehensive research of underlying causes, offering solution-oriented legal recommendations to lawmakers, the diplomatic community, and relevant stakeholders.

It also serves as a platform for the intellectual exchange of perspectives and to have their work published and recognized.

## ABOUT KAS FOR LEGAL YOUTH (KASFLY)

Since its establishment in 2017, KASFLY (KAS For Legal Youth) stands as the exclusive competency fellowship for students and young professional in the legal field. The program provides them a series of intensive trainings designed to strengthen their critical thinking, research and analysis skills, and academic writing skills. KASFLY program also connects them with government institutions and civil society organizations to learn about the existing mechanism and explore potential avenues for improvement. The program component consists of training with national and international experts, discussion, networking, and study visit. We empower these young leaders to make positive change in legal spectrum through producing Law Brief advocating for effective legal enforcement and pro-bono work like Clinic Legal Education.

If you are interested in the program, please stay tune with the open application in the upcoming year.
For more information, please contact
Sereivathna Bunny
via sereivathna.bunny@kas.de

**Editors**
**PAUL MORNET**
SEREIVATHNA BUNNY

**Proofreading By**
BUNTHEOURN SREYKUN

**Layout Design**
TANN SOPHEAVY

**Disclaimer**

The designated contributions do not necessarily reflect the opinions and views of the editorial team and the Konrad-Adenauer-Stiftung or Royal University of Law and Economics. Hence, assumptions made in the articles are not reflective of any other entity other than the author(s) themselves—following, they may be opinionated and subject to revision as well.

KONRAD ADENAUER STIFTUNG

## ABOUT KONRAD-ADENAUER STIFTUNG

Freedom, justice, and solidarity are the basic principles underlying the work of the Konrad-Adenauer-Stiftung (KAS). KAS is a political foundation, closely associated with the Christian Democratic Union of Germany (CDU). As co-founder of the CDU and the first Chancellor of the Federal Republic of Germany, Konrad Adenauer (1876-1967) united Christian-social, conservative and liberal traditions. His name is synonymous with the democratic reconstruction of Germany, the firm alignment of foreign policy with the trans-Atlantic community of values, the vision of a unified Europe, and an orientation towards the social market economy. His intellectual heritage continues to serve both as our aim as well as our obligation today. In our European and international cooperation efforts, we work for people to be able to live self-determined lives with freedom and dignity. We make a contribution underpinned by values to help Germany meet its growing responsibilities throughout the world.

KAS has been working in Cambodia since 1994, striving to support the Cambodian people in fostering dialogue, building networks, and enhancing scientific projects. Thereby, the foundation works towards creating an environment conducive to social and economic development. All programs are conceived and implemented in close cooperation with the Cambodian partners on central and sub-national levels.

Learn more through KAS Cambodia Website.

## ABOUT ROYAL UNIVERSITY OF LAW AND ECONOMICS

The Royal University of Law and Economics (RULE) is the first higher education institution in Cambodia. It was originally founded in 1949 as the National Institute of Law and Economics, and then it was renamed as the Faculty of Law and Economic Sciences and integrated into the University of Phnom Penh in 1957. The university was closed during the Khmer Rouge Regime (1975-1979), and re-opened in 1982 as the Administrative and Judicial School and then the Royal University of Law and Economics in 2003.

RULE currently has four faculties (the Faculty of Law, the Faculty of Public Administration, the Faculty of Economics and Management, and the Faculty of Informatics Economics) and a Dual Degree Department proposing dual bachelor's and master's programs in law and economics with partner universities located in Western Europe, including an international faculty comprising of tenured professors from world's leading universities, participating in RULE's internationalization strategy.

The university currently welcomes over 19,000 students, mostly enrolled in law programs, a number in constant expansion as a testimony of the quality of its academic offer and the dynamism of the high education sector in Cambodia. For more information, visit RULE general website
https://rule.edu.kh/en/ or the Dual Degree Department website https://ddprule.org/

# EDITORIAL NOTE

Cambodia is undergoing a swift digital revolution, which has prompted lawmakers to draft several standalone legislations and subsequent regulations to ensure these changes benefit innovation and productivity while safeguarding individual safety and privacy, a delicate balance when considering the manifold constraints stemming from fast-paced developments, resulting in uncertainty and limited competencies. This publication aims to shed light on some of these legal changes, offering insights to support informed public debate. It focuses on five main areas: data protection, intellectual property law and digitalization, digital markets law, cybercrime law, and law and AI, richly covering a wide range of sub-themes. Each contribution is organized around a narrow, well-defined problem of law that is contemporary and relevant to stakeholders accompanying this ongoing legislative effort, to identify and dissect the various competing solutions, and ultimately propose a superior solution adapted to the Cambodian technological, economic, and legal context. Comparative analysis occupies an important place in the legal reasoning that constitutes each brief, as it enriches analysis through meticulous observations of the legal decisions made by foreign legislators and their impacts. Additionally, it considers the various inspirations drawn from foreign legal systems, particularly that of the European Union, by Cambodian legal teams.

Readers should be reminded about the particular profiles of the young authors behind these law briefs and the circumstances that have led them to dedicate a significant amount of time to researching and analyzing this wide array of topics. Having been carefully recruited by KAS FLY team, these young apprentice lawyers, most of them registered in a bachelor's degree in law at major Cambodian universities, have been trained as KAS FLY fellows for a total of six months, attending various lectures and trainings dedicated to digital law and legal reasoning. The objective was to accompany them in the drafting process of their first publication, with strict qualitative thresholds and personalized support. My view as editor is that most fellows have demonstrated the capacity to move beyond the descriptive habits generally found at this stage of academic development toward embracing analysis, a perilous and demanding journey. The quality of the drafts has largely improved after three different submissions over a period of three months. Nevertheless, please note that your constructive criticism and enquiries are sought to initiate debates on such important topics and nurture the academic excellence of Cambodia's legal youth. I wish you a pleasant reading.

**PAUL MORNET**
Program Director
RULE Dual Degree Department in Law

# CONTENTS

Editorial Note ..... 4
*PAUL MORNET*
*Program Director, RULE Dual Degree Department in Law*

**Section 01: Data Protection Law** ..... 7

Line of Authority: Jurisdictional Challenges in Cambodia's Data Protection Landscape - **KOEUT Sokunkosoma** ..... 8

Strengthening Children's Personal Data Protection on Social Media in the Cambodian Context: A Legal Analysis of Vulnerable Data Subjects and Special Protections - **PROM Sovanita** ..... 14

Safeguarding Privacy, Enabling Access: Regulating Encryption in Cambodia's Digital Era - **MEAN Sopordaliss** ..... 22

Biometric Data: Balancing Digital Innovation with Privacy Rights in Cambodia - **LIM Yseang** ..... 29

Enhancing Oversight on Cambodian Personal Data: Adequacy Decision On Cross-Border Data Transfers to the European Union - **SUN Neakputhkun** ..... 36

Bridging the Gap: Toward a Legal Framework for the Right to Erasure in Cambodia's Digital Age - **TENG Solisa** ..... 43

**Section 02: Intellectual Property Law and Digitalisation** ..... 50

The Absence of Legal Recognition and Enforcement Mechanisms for Publicity Rights in Cambodia's Digital Sphere - **RATANAK Prathnapitou** ..... 51

'The Copyright Dilemma: a Critical Approach to Ownership of AI-Generated Content - **CHES Sindy** ..... 58

**Section 03: Digital Markets Law** ..... 67

Tackling Subscription Trap in Cambodia's E-Commerce Sector: Issues of Automatic Renewals and Free Trial Conversions - **KOEUNG Kimhab** ..... 68

'Monetisation and randomness of the rewards mechanics – interpreting loot boxes as gambling? - **PRUM Sopheareach** ..... 76

From Silence to Consent? A Legal Analysis of Advertising Communications: A Comparison of the Cambodian, Singaporean and European Frameworks- **LIM Yseang** ..... 85

Legal Challenges on Consumer Protection in E-Sport Sector in Cambodia: Challenges and Solutions - **SIM Sokchantepy** ..... 93

**Section 04: Cybercrime Law** ..... 99

From Bytes to Burden of Proof: Establishing Cambodia's Digital Evidence Framework - **ODOM Somnang** ..... 100

Delimiting freedom of expression in Deepfakes: Tackling Malignant Deepfake Personality Rights Violation in Identity Theft and Non-Consensual Intimate Imagery Deepfakes - **RATTANA Sokunthyda** ..... 107

**Section 05: Law and AI** ..... 115

Future of AI Liability Regulation in Cambodia: Insights from the Implications of the European Union's Withdrawal of the AI Liability Directive - **SON Solita** ..... 116

Discriminatory Risks of Predictive Artificial Intelligence and Inferences of Sensitive Personal Data: Considerations for Cambodia - **HENG Sirimongkul** ..... 123

# Section 01

# Data Protection Law

# Line of Authority: Jurisdictional Challenges in Cambodia's Data Protection Landscape

**KOEUT Sokunkosoma**

[Senior law student at ELBBL of RULE]

She has participated in the 21st Willem C. Vis East International Commercial Arbitration Moot. Receiving the David Hunter Award Best Written Memorandum for Claimant amongst 144 participating teams, and the 19th LAWASIA International Moot Competition. Previously, she had completed an internship for the English Language Based Master of Law Program.

## I. Introduction

Regulating personal data and telecommunication is faced with unavoidable scrutiny, one of which is the clarity of the role being appointed. Through the preservation of academic insight, institutional conflicts among regulatory authorities are prominent in developing societies.[1] These tensions are driven by evolving legal structure,[2] and constrained institutional capacity. Within this context, the Law on Telecommunication designates the Telecommunication Regulator of Cambodia (**TRC**) as the supervisory body to oversee the telecommunication industry. TRC holds the position to regulate the telecommunication service, enforcing compliance and maintaining the service integrity.[3] As such, the obligation would extend to the issue of data protection due to the nature of telecommunication data. In parallel to this, Cambodia is currently in the process of establishing a Personal Data Regulator (**PDR**) under the Personal Data Protection Law **(PDPL)**.[4] The co-existence of two regulatory bodies, where one regulates telecommunication services and another oversees matters of personal data protection, creates a potential jurisdictional ambiguity and regulatory overlaps.[5] This may lead to inefficiencies in compliance, with a conflict of the regulatory standards.

[1] Sothie Keo, Sophearatha Ros, "Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia," in Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond, eds. Phallack Kong, Thomas Honnet (Phnom Penh, Cambodia: Konrad-Adenauer-Stiftung, Royal University of Law and Economics, and National University of Management, 2023), pp.41-51.
[2] Ibid.
[3] Law on Telecommunications, Royal Decree NS/RKM/1215/01. December 17, 2015, Articles 5(7)&12.
[4] Phallack Kong, "Developing a Comprehensive Personal Data Protection Framework for Cambodia," in Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond, eds. Phallack Kong, Thomas Honnet (Phnom Penh, Cambodia: Konrad-Adenauer-Stiftung, Royal University of Law and Economics, and National University of Management, 2023), pp.19-25.
[5] Georgios Leris, Adam Copeland, "Telecoms, Media and Internet Laws and Regulations USA 2025," International Comparative Legal Guides, December 17, 2024, https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/usa (accessed March 21, 2025).

Stemming from a fragmented legal landscape that could materialize into a prolonged and complex resolution.[6] Likewise, this paper shall explore the challenges arising from the co-existence of TRC and PDR, scoping on the four interconnected sub-problems: (**II**) Regulatory Collision in Data and Telecommunication Oversight, (**III**) Conflict in Compliance Standard and Regulatory Requirements (**IV**) Dispute resolution and Consumer protection Challenges, and (**V**) the Lack of Coordinated Supervisory Oversights.

# II. Regulatory Collision in Data and Telecommunication Oversight

TRC is empowered to Audit,[7] investigate, and sanction the telecommunication provider.[8] Meanwhile, the PDR would possess the authority to follow a similar, if not identical, authority when personal data is involved.[9] This indicates duplication of oversight, which may create uncertainty for both the regulators and other related entities.[10]

Under the European Union, it offers a comparative model under the provision of Article 60 General Data Protection Regulation (**GDPR**), whereby it establishes a Lead Supervisory Authority (**LSA**). Empowering it to coordinate with other related authorities, in a format of information sharing across jurisdictions.[11] Furthermore, the GDPR embodies the principle of subsidiarity by prioritizing decision-making at the national level,[12] wherever effective.[13] This could be inferred through the National Data Protection Authorities (**DPAs**) to cooperate directly in managing cross-border cases.[14] Such action minimized duplication, indicating clear procedural rules for cases beyond the country border.[15] Despite this effort, some shortcomings remain. As seen in the Digital Service Act, the centralized enforcement authority for large online platforms, "VLPOs" and search engines, "VLOSEs" in the European Commission (**EC**).[16] Provided under the Digital Service Act, the Digital Services Coordinators could only act if the EC has failed to take enforcement action against a potential breach. Such a shift raises concerns about the regulatory independence of the EC, as not an independent regulator but the EU's executive body.[17] Thereby, indicating that the commission's dual roles as both the policy-maker and enforcer may undermine the Digital Service Act's legitimacy.

On the other hand, as seen in the Australian Law Reform Commission's (**ALRC**) report, which detailed how it handles network-level security breaches. This is with the involvement of other key regulators such as the Office of Privacy Commissioner, the Australian Communications and Media Authority, and the Telecommunications Industry Ombudsman. The ALRC recommends that a Memorandum of Understanding (**MoU**) be established. In order to effectively coordinate the delineation with the responsible authority in the conduct of information sharing and referral protocol.[18]

[6] Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)," International Journal of Law and Information Technology 18, no. 2 (Summer 2010): pp.176-193.
[7] Law on Telecommunications, Royal Decree NS/RKM/1215/01. December 17, 2015, Articles 5(7) &10-12.
[8] Ibid.
[9] Phallack Kong, "Developing a Comprehensive Personal Data Protection Framework for Cambodia," op. cit., pp.22-24.
[10] Law on Telecommunications, Royal Decree NS/RKM/1215/01. December 17, 2015, Article 5(7).
[11] GDPR.expert, "Article 62: Joint Operations of Supervisory Authorities - GDPR.expert," https://www.gdpr-expert.com/article.html?mid=5&id=62#eu-regulation (accessed February 14, 2025).
[12] George A. Bermann, "Subsidiarity and the European Community," Hastings International and Comparative Law Review 17, no. 1 (1993): pp.97-120.
[13] European Parliament. "The Principle of Subsidiarity." Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/sheet/7/the-principle-of-subsidiarity (accessed February 3, 2025).
[14] Els De Busser, "Data Protection Around the World: Belgium," in Data Protection Around the World: Privacy Laws in Action, ed. Elif Kiesow Cortez (Hague, Netherlands: T.M.C Asser Press, 2021), p.20.
[15] Victoria Hordern, "Ireland's Approach to Enforcing the GDPR," Taylor Wessing, February 13, 2023, https://www.taylorwessing.com/de/global-data-hub/2023/february---gdpr-enforcement/irelands-approach-to-enforcing-the-gdpr.
[16] Ilaria Buri, "A Regulator Caught Between Conflicting Policy Objectives," Verfassungsblog, October 31, 2022. https://doi.org/10.17176/20221031-220451-0.
[17] Ibid.
[18] Australian Law Reform Commission, Review of Australian Privacy Law, DP 72 (2007), Proposal 64–5.

Thus, putting the effort that ensure efficient collaboration and a clear line of expertise.[19]

Here, adopting a similar means of collaboration between the TRC and the PDR could be beneficial. The process itself could be formalized through the delineation of responsibilities through the process of an MoU, or an inter-agency coordinated framework. With this, the identification of the primary and secondary roles could easily be found based on the nature of the case. For instance, a case involves both the integrity of the telecommunication infrastructure and personal data processing. A joint task force or shared jurisdiction could then be invoked. Amendment of the obligation could be made via the sub-decree.[20] Outlining the cooperative mechanisms, showcasing the importance of delineations of when responsibilities naturally intersect.

# III. Conflict in Compliance Standards and Regulatory Requirements

Potential Clash in compliance standards could take place, considering that the TRC already imposes sector-specific compliance on the telecommunications service providers.[21] The concern would be that once the PDR begins enforcing the Personal Data Protection Laws. The telecommunications operators would find themselves subject to two sets of overlapping, conflicting obligations. Likewise, a jurisdiction that emphasizes the balanced trust within the digital economy.[22] Both with the intention to safeguard accountability and data management.[23] Singapore maintains the separation between data protection and telecommunications by creating a structured mechanism for cooperation.[24] Given that Personal Data Protection Commission (**PDPC**),[25] is administratively housed under Infocomm Media Development Authority (**IMDA**),[26] being part of the Ministry of Digital Development and Information.[27] This makes it possible for the arrangement of regular communication and cross-agency alignment. Especially for regulatory issues that span both data protection and service delivery. Thus, indicating that PDPC still retains its power to enforce the provisions from the Personal Data Protection Act (**PDPA**), for conditions such as purpose limitation, and data breach notification requirements.[28] This is through coordinating with the IMDA when telecom-specific technical standards or infrastructure considerations are involved.[29] Thereby, PDPC and IMDA could conduct a joint assessment or parallel investigation, allocating a clear line of delineated scope of authority.[30] Notably, the PDPC has issued sector-specific advisory guidelines in consultation with the IMDA, helping the telecom operators to synchronize their operations.[31] This is while being cautious of both data protection and telecom regulatory standards, to avoid a contradictory set of instructions.[32]

The same scenario could play out in a manner where the TRC may require the service provider to store communication records for a specified period for law enforcement purposes.[33]

[19] Webadmin, "Telecommunications Regulators," ALRC, August 17, 2010. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/73-other-telecommunications-privacy-issues/telecommunications-regulators-2/.
[20] Law on Telecommunications, Royal Decree NS/RKM/1215/01. December 17, 2015, Article 13.
[21] Law on Telecommunications, Royal Decree NS/RKM/1215/01. December 17, 2015, Articles 12&56.
[22] Lim Chong Kin, Anastasia Su-Anne Chen, "Data Protection Laws and Regulations Singapore 2024-2025," International Comparative Legal Guides International Business Reports, July 31, 2024, https://iclg.com/practice-areas/data-protection-laws-and-regulations/singapore.
[23] Ibid.
[24] Ibid.
[25] Personal Data Protection Act 2012, No. 26 of 2012 (20th November 2012); Personal Data Protection (Amendment) Act 2020, No. 40 of 2020 (25th November 2020).
[26] Lim Chong Kin, Anastasia Su-Anne Chen, "Data Protection & Privacy - Singapore," in Lexology GTDT Data Protection & Privacy 2023, consulting editors Aaron P. Simpson and Lisa J. Sotto (London: Law Business Research, 2023), pp.6-7.
[27] Lim Chong Kin, Anastasia Su-Anne Chen, "Singapore: EU Cooperation and AI Governance Testing Keep City State at the Cutting Edge," in GDR Insight Handbook (Drew & Napier LLC, 2024), pp. 76-77.
[28] PDPA 2012, 2020 Rev. ed., section 10.
[29] Lim Chong Kin, Anastasia Su-Anne Chen, "Data Protection & Privacy - Singapore," op. cit., pp.11-12.
[30] PDPA 2012, 2020 Rev. ed., section 10.
[31] Personal Data Protection Commission (PDPC), Advisory Guidelines for the Telecommunication Sector, https://www.pdpc.gov.sg/guidelines-and-consultation/2017/10/advisory-guidelines-for-the-telecommunication-sector (accessed April 11, 2025); Lim Chong Kin, Anastasia Su-Anne Chen, "Data Protection & Privacy - Singapore," op. cit., p.5.
[32] Ibid.
[33] Prakas No. 228 on the Operations of the International Telecommunications Gateways.

As such, TRC may approve cross-border data transfers based on operational needs,[34] whereas the PDR may impose stricter safeguards and conditions.

In a nutshell, these discrepancies could cause compliance uncertainty and could increase the operational costs and hinder effective regulatory adherence. The legislator may consider aligning the data protection obligation with sector-specific rules in a format that reduces misalignment and avoids contradiction.[35] By handling the dispute systematically rather than through means of *ad hoc*.[36] This is possible, given that a similar mechanism was established in the Inter-Ministral Prakas No. 170 on the Management of dissemination via websites and social media networks operating through the internet in the Kingdom of Cambodia. The proclamation outlines the role of Ministries that have the obligation to regulate online media and social media content within Cambodia. Those bodies being the Ministry of Post and Telecommunications (**MPTC**), the Ministry of Interior, and the Ministry of Information, who would operate their duty through their specialized units and measures.[37] As the MPTC holds the central role of drafting the Personal Data Protection Law,[38] and possesses the regulatory authority within the telecommunication sectors through the TRC.[39] The MPTC possesses a discretionary role within digital governance.[40] Therefore, it could coordinate a joint dispute mechanism for cases that may invoke issues of regulatory disagreements.

# IV. Dispute Resolution and Consumer Protection Challenges

Despite the main emphasis of the issue being that of the jurisdictional challenge, which has an impact on institutions, the same greatly affects the public. In the event of a data breach committed by the telecom operator, the consumer may face uncertainty on whether to approach the TRC for service-related issues or the PDR for data-related grievances. The anticipated confusion could undermine trust in the regulatory process. Discouraging the affected individuals from seeking justice. This is particularly frustrating considering Cambodia's limitations in both digital literacy and legal awareness.[41]

In contrast to this, Article 65 GDPR simplifies the concern by the establishment of dispute resolution amongst the supervisory authorities when disagreements arise over the regulatory decisions.[42] The concerned supervisory authority possesses the right to raise an objection to the LSA's draft decision.[43] After which the matter shall be referred to the European Data Protection Board, which will issue a binding decision to resolve such matter.[44] This undergoes the process by which the Union takes over the case when it is seen that the member cannot effectively achieve the goal of addressing the case on their own.[45]

[34] Ibid.
[35] Inter-Ministral Prakas No. 170 on the Management of dissemination via websites and social media network operating through the internet in the Kingdom of Cambodia; Inter-Ministral Circular No. 001 on Bussiness Managment and the use of Telecom Service.
[36] Ibid.
[37] Ibid.
[38] Sothie Keo, Sophearatha Ros, "Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia," op. cit., p.44.
[39] Law on Telecommunications, Royal Decree NS/RKM/1215/01. December 17, 2015, Article 6.
[40] Sub-Decree No. 110 ANKr.BK on the Authorization to Operate Information and Communications Technology, July 21, 2017.
[41] Phallack Kong, "Developing a Comprehensive Personal Data Protection Framework for Cambodia," op. cit., p.23.
[42] European Data Protection Board, Guidelines 09/2020 on Relevant and Reasoned Objection Under Regulation 2016/679 (Brussels: European Data Protection Board, 2020), pp.2-8.
[43] Ibid.
[44] Ibid.
[45] Michelle Dr. Evans, "The Principle of Subsidiarity in European Union Law: Some Comparisons with Catholic Social Teaching," Solidarity: The Journal of Catholic Social Thought and Secular Ethics 3, no. 1 (ResearchOnline@ND 2013): pp.69-72.

In that sense, Cambodia can approach this by creating a joint grievance resolution committee involving both the TRC and PDR. The committee could be in charge of reviewing complex complaints and determining the jurisdictional responsibility based on the predefined criteria provided by the law.[46] Here, instead of introducing more layers of regulatory bodies, the effort should focus on enhancing the accessibility and clarity of the existing mechanism. Though the initiation of a central digital portal for the filing of data protection complaints could potentially help to streamline resolution pathways, reduce administrative burden, and increase transparency over the process. Nevertheless, an effective implementation is not plausible without first addressing the issue of resource constraints,[47] institutional competency, and ensuring the regulator's independence.

# V. Lack of Coordinated Framework and Supervisory Oversight

The threshold of this issue is not unique to the digital landscape; similar overlaps have been observed in other sectors. Such as between the Consumer Protection Competition and Fraud Repression Directorate-General and the Anti-Cyber Crime Police on matters of false advertisement,[49] and digital fraud. Though affected individuals can file complaints with either authority, doing so may result in duplication of effort, being inefficient for resolution being enforced. As such, responsibility shall hinge upon the status of the business registration license with the MOC.[50] If it is found to be unregistered, then the case falls under the Anti-Cyber Crime Police's authority. This distribution of authority, though aimed at specialization, may fragment enforcement and create jurisdictional confusion.[51] Legislators are likely to include provisions in the Personal Data Protection Law for the supervisory coordination.[52] Through an inter-agency council chaired by the MPTC with representatives from TRC and PDR, and other related entities, to standardize procedures and resolve disputes.

Likewise, a jurisdiction that prioritize national security, such as China's Cyberspace Administration of China (**CAC**), which serves as the centralized authority that oversees multiple dimensions of digital governance.[53] This includes data protection, cybersecurity, and online content regulation. The CAC was established with the mandate to handle violations, conduct investigations, and issue binding instructions.[54] In its early years of establishment, the CAC also faced with issue of overlapping functions and occasional institutional tension with other regulatory bodies, notably the Ministry of Industry and Information,[55] the Ministry of Public Security, and the State Administration for Market Regulation.[56] The interaction could play out in a variation where the Ministry of Industry and Information, known as the principal regulator for the telecommunications industry.[57]

[46] Phallack Kong, "Developing a Comprehensive Personal Data Protection Framework for Cambodia," op. cit., p.19.
[47] Sothie Keo, Sophearatha Ros, "Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia," op. cit., p.51.
[48] Ibid.
[49] Law on E-Commerce, Royal Decree NS/RKM/1119/017, November 2, 2019; Prakas No. 185 on Information Standards for Consumer, Articles 6;8&9.
[50] Law on E-Commerce, Royal Decree NS/RKM/1119/017, November 2, 2019, Article 26; Sub-Decree No. 84 ANKr.BK on Business Registration through Information Technology System, Articles 3&9.
[51] Sothie Keo, Sophearatha Ros, "Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia," op. cit., p.45.
[52] Inter-Ministral Circular No. 001 on Bussiness Managment and the use of Telecom Service.
[53] Rogier Creemers, "China's Emerging Data Protection Framework," Journal of Cybersecurity 8, no. 1 (2022): tyac011.
[54] Ibid.
[55] Mark Parsons, Sherry Gong, and Tong Zhu, "China's CAC and MIIT Undertake Parallel Consultations on Draft Measures for Cyber Incident Reporting," Hogan Lovells, January 24, 2024, accessed February 17, 2025, https://www.hoganlovells.com/en/publications/chinas-cac-and-miit-undertake-parallel-consultations-on-draft-measures-for-cyber-incident-reporting#:~:text=Implementation.
[56] Oscar Wang, Yuri Van Der Leest, and Devin Mullin, "China Cybersecurity and Data Regulation: What Multinationals Should Know," Teneo, October 25, 2021, https://www.teneo.com/insights/articles/china-cybersecurity-and-data-regulation-what-multinationals-should-know/.
[57] Jamie P. Horsley, "Behind the Facade of China's Cyber Super-Regulator," DigiChina, August 8, 2022, https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/ (accessed February 27, 2025).

Overseeing the network infrastructure, technical standards, and licensing. Similarly, the State Administration for Market Regulation was mandated to oversee data-related aspects of consumer protection and market conduct. As China's digital government evolves, the conflict has become more evident, which is related to the introduction of the data governance legislation. Such as the Cybersecurity Law (2017), the Data Security Law (2021) and the Personal Information Protection Law (**PIPL, 2021**), which prompted institution restructuring and a formal delineation of responsibilities. The Chinese government then elevated the CAC's status by making it the *de facto* authority, being responsible for coordination, enforcement, and policy implementation. This is by way of reinforcing the declaration that the CAC be the lead agency and acting in support of other sector-specific capacities.

Cambodia could opt for a similar model featuring central coordination, rapid response protocols, and a specialized enforcement unit. Being tasked to develop a national compliance framework by ways of integrating cross-sector obligations and clarifying the regulatory hierarchy with proportional safeguards. A formal inter-agency coordination between TRC and PDR could reduce the conflicting norms. Furthermore, the Legislator may consider having a legislative clarification, explicitly naming PDR as the primary enforcement body, while delegating auxiliary roles to other agencies based on technical or sectoral expertise. Given that the PDR would likely make reports directly to the MPTC, being the body of authority with the highest level in the state hierarchy. Such evaluation helps to resolve the inter-agency dispute swiftly through the means of aligning the regulatory priorities with the national strategic goals.

# VI. Conclusion

Overall, the intersection of Cambodia's telecommunication regulation and personal data protection presents a rich discussion on the expectations of the upcoming regulation. Throughout, we see that each component of this paper explored issues of ambiguity on a jurisdictional basis, potential frustration of the complaint standard, the protection of the consumer hurdles, with a fragmented framework that did not provide coordinated oversight. This reveals an in-depth debate on the institutional overlap between the TRC and PDR, generating legal and operational uncertainties. Given that these regulators are poised to operate concurrently. The mandate being given would intersect in the governance of telecommunication data, outlining concerns about regulatory clarity and the efficiency of their operation. Likewise, by synthesizing the core findings of the issue. We see that Cambodia requires not only regulatory innovation but an effective institutional collaboration. While the proposal of an entirely new authority or paradigm is not prohibited. It is recommended that mechanisms such as an MoU, joint compliance, and an inter-agency council are to be the preferred means to potentially resolve the issue and enforce a coherent standard. The interference could be drawn upon by the GDPR or other lead supervisory authorities, such as the CAC and PDPC. With these improvements, Cambodia can move forward with the reassurance that the regulatory community has properly engaged in the exploration of formalized inter-agency frameworks. National compliance and structures that reduce fragmentation.

[58] Ibid.
[59] Paul Triolo, Samm Sacks, Graham Webster, and Rogier Creemers, "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus," DigiChina, August 18, 2021, https://digichina.stanford.edu/work/after-5-years-chinas-cybersecurity-rules-for-critical-infrastructure-come-into-focus/.
[60] Freedom House, "China," Freedom House, n.d., https://freedomhouse.org/country/china/freedom-net/2022#footnote7_fNuVvSArVQIns5nEOX5PmSligabSVE2Do6tW97o--Y_n7nKOHZzoZd8 (accessed April 27, 2025).
[61] Rogier Creemers, China's Cyber Governance Institutions, LeidenAsiaCentre Report, 2022, https://leidenasiacentre.nl/en/report-chinas-cyber-governance-institutions/ (accessed April 27, 2025).
[62] Sothie Keo, Sophearatha Ros, "Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia," op. cit., pp.44-45.

# Strengthening Children's Personal Data Protection on Social Media in the Cambodian Context: A Legal Analysis of Vulnerable Data Subjects and Special Protections

**PROM Sovanita**

[Sophomore in dual-degree law program at the American University of Phnom Penh]

Through her role as the finance and public relations executive in the Debate Society and Raymond Leos Law Society at AUPP, she demonstrates versatility across diverse organizational environments. Currently, she is competing in the 4th National Commercial Arbitration Centre (NCAC) Arbitration Moot Competition driven by her keen interest in commercial arbitration and commercial law, and she is also interning at DFDL's real estate and construction practice group.

## I. Introduction

The increased presence of Cambodian children and adolescents on social media platforms poses distinct vulnerabilities,[1] demanding legal recognition to distinguish these age groups.[2] While young children are particularly vulnerable to online risks due to limited cognitive capacity and dependence on parental consent,[3] adolescents encounter equally challenging issues triggered by their online engagement from personal data (e.g., identity, location, opinion, appearance) shared online.[4] Combined with the gap in digital literacy rates across various socio-economic backgrounds in Cambodia, this hinders children and parental guardians' ability to recognize and mitigate online risks safely and effectively.[5] Pursuant to Article 3 of the Convention on the Rights of the Child (**UNCRC**), prioritize the best interests of children.[6] Not only protecting younger children, but also recognizing the evolving capacities and digital maturity of adolescents.[7]

Currently, the absence of adequate safeguards for Cambodian children's personal data protection demands a clear distinction of age limits and special protection. Therefore, this brief aims to examine the distinct vulnerabilities of children and adolescents on social media,

[1] Ministry of Post and Telecommunications (MPTC), Cambodian Child Online Protection Guidelines for the Digital Technology Industry (Phnom Penh: UNICEF Cambodia, 2023), 4.
[2] Patricia Boshe, "A Thought on Child's Best Interest in Data Protection," in Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond, ed. Kong Phallack and Thomas Honnet (Phnom Penh: Konrad-Adenauer-Stiftung, 2023), 85–101.
[3] Christopher Jones, "Balancing the Autonomy and Protection of Children: Competency Challenges in Data Protection Law," Information & Communications Technology Law (2024): 1, https://www.tandfonline.com/doi/full/10.1080/13600834.2024.2320978.
[4] PUNICEF, The State of the World's Children 2017: Children in a Digital World (New York: UNICEF, 2017), 30.
[5] MPTC, Cambodian Child Online Protection Guidelines, 34.
[6] Convention on the Rights of the Child, G.A. Res. 44/25, U.N. Doc. A/RES/44/25 (Nov. 20, 1989), Article 3.
[7] Organization for Economic Co-operation and Development (OECD), Recommendation of the Council on Children in the Digital Environment, C(2021)64 (Paris: OECD Publishing, 2021), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389.

recommend a tiered age of digital consent, and conduct a comparative analysis of the existing Cambodian civil code with influential international standards that have adopted approaches for children and adolescents for the upcoming "Personal Data Protection Act (**PDPA**)". This comparison will focus on differentiated ages of consent, parental rights, corporate compliance and enforcement, including judicial oversight.

# II. Setting Triered Threshold: The Age of Digital Consent in Cambodia

Establishing a single age threshold is insufficient to address the vulnerabilities of children on digital platforms, not only of children but also of adolescents.[8] These distinctions are important to legally know when these age groups are capable of consenting to the processing of their personal data online.[9] Below the age threshold, it is widely recognized that parental or legal guardian consent is required for the processing of the child's personal data due to their online exposure to alarming threats, such as sexual exploitation, cyberbullying, data breaches, etc.[10]

While the universal age of digital consent varies across influential jurisdictions, such as the General Data Protection Regulation (**GDPR**) and the Children's Online Privacy Protection Act (**U.S. COPPA**), these jurisdictions have diverse approaches in tackling limited children's capacity.[11] The GDPR sets its threshold to 16 years but allows member states to legislate a minimum age of no younger than 13; this age range allows for prioritizing children's best interests.[12] Conversely, the U.S. COPPA mandates operators of commercial online services to obtain verifiable parental consent before collecting and processing children's personal data under 13 years.[13]

However, models with a singular age of consent overlook the vulnerability of adolescents, because these age groups are neither children nor adults.[14] This has been addressed in the Brazilian General Data Protection Law (**LGPD**), Article 14, which regulates not only the processing of children's data but also that of adolescents in their best interest.[15] Therefore, it is recommended for the upcoming PDPL to distinguish between two thresholds: child and adolescent, allowing the law to fully encompass appropriate protection across developmental stages.

[8] Sonia Livingstone et al., "There is no right age! The search for age-appropriate ways to support children's digital lives and rights," Journal of Children and Media (published online January 7, 2025): 1–19, https://www.tandfonline.com/doi/full/10.1080/17482798.2024.2435015.
[9] UNICEF. "Drawing a Line in Digital Spaces: Age-Based Restriction of Social Media." Policy Note. UNICEF, April 2025. https://www.unicef.org/media/170666/file/Policy%20note_age%20restrictions%20social%20media-new.pdf.
[10] European Parliament Research Service. "Protecting Children Online." Briefing. European Parliament, January 2025. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI(2025)769570_EN.pdf.
[11] Sonia Livingstone, Mariya Stoilova, and Jo Warby. "A Complex Web of Factors Influence Children's Commercial Media Literacy." LSE Business Review, July 22, 2017, https://eprints.lse.ac.uk/83844/1/businessreview-2017-07-22-a-complex-web-of-factors-influence.pdf.
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 8, recital 38.
[13] Federal Trade Commission. "Children's Privacy." Federal Trade Commission, n.d. Accessed May 14, 2025. https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy.
[14] Boshe, "Child's Best Interest," 99.
[15] LGPD Brazil. "Article 14: Personal Data of Children and Adolescents - Chapter 2." LGPD Brazil, n.d. Accessed May 23, 2025. https://lgpd-brazil.info/chapter_02/article_14.

## 1. The Child Threshold: Individuals Under 16 Years Old

For the purposes of the upcoming PDPL, a child is an individual under 16 years old.[16] This alignment is evident in the U.S. COPPA and the GDPR, which establish a lower age threshold for stricter protection.[17] This is also consistent with the upcoming PDPL, which is predicted to set this age threshold. Therefore, data controllers offering services to this age group are obligated to implement verifiable mechanisms easily understood by children and obtain genuine parental consent adhering to the paramount principle of the child's best interest,[18] the law must also include explicit exceptions for instances where obtaining parental consent is unfeasible or could endanger the child, particularly in dire circumstances as such exceptions are waived in jurisdictions like South Africa's Protection of Personal Information Act (**POPIA**).[19] When parental consent might be impossible to secure in a life-threatening emergency (e.g., medical history, emergency contacts) is vital to save a child's life or health, the consent requirement must be waived.[20] Similarly, in the situation of abuse or neglect by the very individual meant to grant consent to the personal data of the child,[21] the requirement of parental consent would block the child from necessary help and accessing essential protection from authority figures.[22] Consequently, this nuanced approach is vital because prioritizing parental consent could, under critical circumstances, block younger children from accessing safe and effective protection they need.[23]

## 2. The Adolescent Threshold: Individuals Aged 16 to 21 Years Old

An adolescent is defined as an individual aged 16 to 21 years.[24] While they possess a greater capacity for understanding and decision-making about their personal data compared to younger children,[25] the law should permit them to provide direct consent to their data online.[26] However, the data controller must ensure absolute transparency of the data processing, and consent can be easily withdrawn without long-term consequences affecting future career or reputation.[27] The proposed upper age limit of 21 years for the 'adolescent' category is intentionally expansive to account for the complexities of digital maturity, to evaluate online information, and digital citizenship that isn't usually fully developed by the age of 18.[28] While legal maturity is considered 18 years old, even in Cambodia,[29] the transition to full digital independence extends beyond this age, often throughout late adolescence.[30] Though more capable than younger children, this age group requires significant special protection as they seek greater autonomy over their personal data online; they need continued digital literacy development while also becoming financially independent, to protect themselves from targeted advertising profiling for commercial gain, manipulative content by online predators, and fraud.[31] Therefore, protecting young individuals shouldn't cease at 18; this tiered approach

[16] Professor Kong Phallack, "Developing a Comprehensive Personal Data Protection Framework for Cambodia," in The Law Talk Publication: Regulating Personal Data Protection and Cybersecurity, edited by Kong Phallack and Thomas Honnet (Phnom Penh, Cambodia: Konrad-Adenauer-Stiftung, 2023), 21.
[17] Clarip. "GDPR-K: Children's Data and Parental Consent under the GDPR." Clarip, n.d. Accessed May 23, 2025. https://www.clarip.com/data-privacy/gdpr-child-consent/.
[18] UNCRC, Article 3
[19] Protection of Personal Information Act 4 of 2013 (South Africa), sec. 35(1).
[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6.
[21] A. van der Made et al., "Data Research on Child Abuse and Neglect without Informed Consent? Balancing Interests under Dutch Law," European Journal of Pediatrics 175, no. 1 (2016): 133, https://pubmed.ncbi.nlm.nih.gov/26490565/.
[22] American Professional Society on the Abuse of Children (APSAC), "Position Paper." August 16, 2019. Accessed May 23, 2025. https://apsac.org/wp-content/uploads/2023/09/APSAC-Position-Paper-Child-Maltreatment-Aug-16-2019.pdf.
[23] UNCRC, Article 3.
[24] Elena Higley, "Defining Young Adulthood" (DNP Qualifying Manuscripts, University of San Francisco, 2019), https://repository.usfca.edu/dnp_qualifying/17/.
[25] Bette Mathews, "Adolescent Capacity to Consent to Participate in Research: A Review and Analysis Informed by Law, Human Rights, Ethics, and Developmental Science," Laws 12, no. 1 (2023): 2, https://www.mdpi.com/2075-471X/12/1/2.
[26] GDPR, Article 8(1).
[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 7(3), OJ L 119, 4.5.2016, p. 1–88; see also Recitals 32, 42.
[28] Candice L. Odgers and Michaeline R. Jensen, "Adolescent Development and Growing Divides in the Digital Age," Journal of Research on Adolescence 30, no. S2 (2020): 224–31.
[29] Civil Code of Cambodia, Article 17.
[30] Odgers and Jensen, Adolescent Development, 145.
[31] Sonia Carcelén-García, Mónica Díaz-Bustamante Ventisca, and María Galmes-Cerezo, "Young People's Perception of the Danger of Risky Online Activities: Behaviours, Emotions and Attitudes Associated with Their Digital Vulnerability", MDPI 12, no. 3 (2023): 164, https://www.mdpi.com/2076-0760/12/3/164.

acknowledges the ongoing vulnerability and developmental needs of children and late adolescents.[32]

# III. Drawing the Line Between Parental Oversight and Children's Online Data Privacy

The increased presence of Cambodian children and adolescents on social media platforms raises a legal challenge for legitimate parental oversight while balancing children's online privacy. With Cambodian total digital literacy rates of 32% in 2020 and 49% among those under the age of 18 as of 2024, this indicates a lack of profound knowledge to use digital platforms effectively and safely.[33] These factors are heavily enshrined in the lower socio-economic group, who have limited access, which hinders parents' capacity to safeguard children's privacy. [34]

Which enables 'sharenting', the practice of parents sharing personal data about their children online, sometimes without the child's informed consent.[35] For younger children, "sharenting" constitutes a direct infringement upon their reliance on parental consent, creating an irrevocable digital footprint of the narratives, images, and sensitive personal data shaped by their parents, which they cannot object to for future consequences.[36] As parents act as both gatekeepers and narrators of the personal data shared online, sharenting directly impacts children's privacy, not only that of younger children but also of adolescents.[37] For adolescents, parental attempts at "oversight" manifest through the deployment of mediation software applications, such as "Safe Chat,"[38] which originated in the U.S., to filter content deemed harmful, most alarmingly are violence and pornography.[39] Given that adolescents' active engagement often involves them lying about their age online,[40] they seek greater autonomy and perceive surveillance as a restriction on their evolving independence.[41] Which leads to restrictive parenting, prohibiting their children's use of social media, which hinders adolescents' development into a digitally literate and independent citizen, as these skills are fostered through responsible and guided online engagement, not through complete absence.[42]

The urgency of addressing these privacy concerns for both younger children and adolescents is evidenced by UNESCO's "Digital Literacy for Employability and Entrepreneurship among Cambodian Youth" report.[43]

[32] Sonia Carcelén-García, María José Narros-González, and María Galmes-Cerezo, "Digital vulnerability in young people: gender, age and online participation patterns," International Journal of Adolescence and Youth 28, no. 1 (2023): 2287115, https://www.tandfonline.com/doi/full/10.1080/02673843.2023.2287115

[33] UNESCO, "Cambodia launches its first competency framework on Digital, Media and Information Literacy to empower citizens in today's digital society," UNESCO, June 27, 2024, https://www.unesco.org/en/articles/cambodia-launches-its-first-competency-framework-digital-media-and-information-literacy-empower.

[34] Jozef Lukáč, Zuzana Kudlová, Janka Kopčáková, and Peter Gallo, "Impact of Socio-Economic Factors on Digital Literacy and Security," TEM Journal 14, no. 1 (February 2025): 925–932, https://doi.org/10.18421/TEM141-81.

[35] UNICEF, "What you need to know about 'sharenting'," UNICEF Parenting, accessed June 17, 2025, https://www.unicef.org/parenting/child-development/what-you-need-know-about-sharenting.

[36] Stacy Scott and Katie Wilson, "Please Don't 'Like' My Baby Photo: How Sharenting Harms the Child and How the Law Can Help," Emory Law Journal 66, no. 4 (2017): 1121, https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2/.

[37] Greet Ouvrein and Katrien Verswijvel, "Sharenting, Is It a Good or a Bad Thing? Understanding How Adolescents Think and Feel about Sharenting on Social Network Sites," Children and Youth Services Review 104 (2019): 104401.

[38] Zainab Iftikhar, Qutaiba Rohan ul Haq, Osama Younus, Taha Sardar, Hammad Arif, Mobin Javed, and Suleman Shahid, "Designing Parental Monitoring and Control Technology: A Systematic Review," in Human-Computer Interaction – INTERACT 2021, ed. Carmelo Ardito, Rosa Lanzilotti, Alessio Malizia, Helen Petrie, Antonio Piccinno, Giuseppe Desolda, and Kori Inkpen, Lecture Notes in Computer Science, vol. 12935 (Cham, Switzerland: Springer, 2021), 676–700, https://www.researchgate.net/publication/354123198_Designing_Parental_Monitoring_and_Control_Technology_A_Systematic_Review.

[39] Kinga Sorbán, "An elephant in the room—EU policy gaps in the regulation of moderating illegal sexual content on video-sharing platforms," International Journal of Law and Information Technology 31, no. 3 (Autumn 2023): 171, https://academic.oup.com/ijlit/article/31/3/171/7273696.

[40] Kristiina Raudsepp, "Protecting Children's Rights and Best Interests in EU Data Protection Law," European Parliamentary Research Service (EPRS) At a Glance, December 2023, 1, https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.

[41] Ratri Rizki Kusumalestari et al., "Parenting styles and digital literacy: Uncovering their correlation among adolescents," Jurnal Kajian Komunikasi 11, no. 2 (2023): 144.

[42] Sonia Livingstone and Mariya Stoilova, "Parenting in the Digital Age," in The SAGE Handbook of Parenting: Theory, Research, and Practice, 2nd ed., vol. 2, Biology, Cognition, and Socialization of Parenting, ed. Marc H. Bornstein (Thousand Oaks, CA: Sage Publications, 2019), 305.

[43] UNESCO, "Cambodia launches its first competency framework."

| Score Types | Mean | | | St Dev | | |
|---|---|---|---|---|---|---|
| Hardware/ software | High | Uni | EMPL | High | Uni | EMPL |
| Information Literacy | 52.3 | 49.9 | 45.4 | 18.3 | 17.6 | 25.2 |
| Content Creation | 45.3 | 52.9 | 53.1 | 15.4 | 16.5 | 19.2 |
| Content creation | 50.0 | 48.0 | 62.8 | 22.8 | 16.9 | 30.8 |
| Safety | 36.8 | 38.1 | 43.2 | 21.0 | 19.7 | 19.5 |
| Overall | 47.3 | 47.9 | 50.6 | 15.3 | 13.0 | 17.1 |

Source of Figure table: UNESCO Digital Literacy for Employability and Entrepreneurship among Cambodian Youth.[44]

The lower mean scores in the 'Safety' category, ranging from 36.8 to 43.2, illustrate that children themselves also lack a thorough understanding of the implications of sharing their data or having their data shared by others. The current absence of a nuanced approach for Cambodia's children's privacy is inadequate to uphold Article 16 of the UNCRC. As this article affirmed, children as data subjects have the right to privacy from their families in terms of family life, private space, phone calls, or emails.[45] For younger children, their privacy is violated due to direct parental consent without exception, as for adolescents, it infringes upon their evolving autonomy due to restrictive parenting and surveillance of private digital interactions.[46]

Therefore, the legislator shall make sure the PDPL ensures that its provisions enable informed consent based on child-friendly terms and conditions that distinguish children and adolescents as distinct data subjects, by reflecting their differential capacities to give genuine consent for their privacy.

# IV. Invisible Influence of Targeted Advertising on Vulnerable Children on Social Media and Corporate Complaince

Companies actively target vulnerable children, as children can easily consume and be influenced by what they see online.[47] These digital marketing strategies behind social media affect children's rights and development in various forms through cognitive development, economic exploitation,

[44] UNESCO, "Cambodia launches its first competency framework."
[45] United Nations Convention on the Rights of the Child, adopted November 20, 1989, G.A. Res. 44/25, 1577 U.N.T.S. 3 (entered into force September 2, 1990), Article 16, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.
[46] Shannon Sorensen, "Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights," Children's Legal Rights Journal 36, no. 3 (2016): 156.
[47] Saad AIT LAMKADEM and Smail OUIDDAD, "Ethical issues about kids targeting," International Journal of Research and Scientific Innovation 7, no. 12 (December 2020): 37,https://www.researchgate.net/publication/347837203_Ethical_issues_about_children_targeting_2020.

and unwanted exposure.[48] For instance, 81% of parents with children aged 11 years or younger let their kids watch YouTube with a regular habit, and 61% of the parents found inappropriate content on the platform.[49] Furthermore, companies monetize off the utilization of algorithms to target children, ranging from food products such as sweets, toys, and clothing, among others.[50]

However, companies will face limitations in complying with guidelines to protect children, as it is an investment being put into developing separate apps.[51] Social media platforms have tried to introduce their own 'kid' version of the apps, such as YouTube Kids, while Instagram paused its introduction to the kid version of the app and instead values the guidelines on parental supervision and guidance by blocking certain content with age thresholds of under 13 years.[52] This indicates that continuous efforts from the government and relevant stakeholders are crucial to ensure corporate compliance for children's data,[53] especially a robust age verification system through the differentiation of young children and adolescents, and not solely relying on parental consent. But rather to allow children to be autonomous and truthful about their usages, including various methods set forth below:

**1.** Age estimation is the method that allows platforms to provide suitable content by predicting individuals' age from their digital images.
**2.** Age verification is the method of checking an estimated age to set an age limit to allow access to age-restricted services.
**3.** Age comparability is comparing the age of a selfie with the claimed age from an ID. [54]

These issues can be alleviated as it has been acknowledged by the Ministry of Post and Telecommunication in categorizing the risk into content, contact, conduct, and contract risk, moving forward especially for the data controller and processor to take special care with elaborate provisions when it comes to collecting online data of younger children and adolescents.[55]

# V. Judicial Oversight: The Court's Role Regarding Child Digital Consent

Legal framework in establishing the digital age of consent, promoting children's privacy, and ensuring corporate compliance alone cannot fully address the nuances and complexity of children as vulnerable data subjects on social media. Considering the varying degree of digital literacy and socio-economic factors, along with limitations of compliance from corporate entities, makes this a solid ground for judicial oversight. In pursuant with the Cambodian Civil Code, Article 21 allows for the court to declare emancipation for minors aged 16 years or above, if they can demonstrate

[48] UNICEF, Children's Rights and Digital Marketing: A Discussion Paper (New York: UNICEF, 2021), 5, https://www.unicef.org/childrightsandbusiness/media/256/file/Discussion-Paper-Digital-Marketing.pdf.
[49] Michelly Rosa Ferreira and Luísa Agante, "The Use of Algorithms to Target Children while Advertising on YouTube Kids Platform: A reflection and analysis of the existing regulation," International Journal of Marketing, Communication, and New Media (May 2020): 41.
[50] UNICEF, "What you need to know about 'sharenting'."
[51] International Telecommunication Union, Guidelines for Policy-Makers on Child Online Protection (2020), accessed via Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, https://azlp.ba/publikacije/default.aspx?id=3526&langTag=bs-BA.
[52] Adam Mosseri, "Pausing 'Instagram Kids" and Building Parental Supervisions Tools", Instagram, September 27, 2021, https://about.instagram.com/blog/announcements/pausing-instagram-kids.
[53] UNICEF Innocenti Research Centre, The Case for Better Governance of Children's Data: A Manifesto (Florence: UNICEF Innocenti, 2021), https://www.unicef.org/innocenti/media/1031/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf.
[54] François David et al., "JAM: A Comprehensive Model for Age Estimation, Verification, and Comparability," arXiv preprint arXiv:2410.04012 (2024), https://arxiv.org/html/2410.04012v1.
[55] MPTC, Cambodian Child Online Protection Guidelines, 32.

self-sufficiency and it is deemed in their best interest. Article 22 further states that an emancipated minor also possesses the same capacity to act as an adult; this status can be achieved through a court declaration as per Article 21 or automatically upon marriage.[56] These provisions, along with Cambodia's ratification of the Convention on the Rights of the Child (**CRC**), are key principles on the child's right to privacy and the child's best interest, allowing for consideration of judicial decisions.[57] A child's best interest is a legal principle that prioritizes what is best for a child in all aspects, from welfare, safety, well-being, and rights.[58] Therefore, in circumstances where this application applies, judicial decision may override parental or legal guardian consent.

The principle of the child's best interest has also been addressed in other jurisdictions, overriding parental and legal guardian consent as seen in Algeria and Tunisia.[59] Algeria requires consent from a legal authority; otherwise, authorization from competent judges is necessary.[60] Similarly, in Tunisia, the processing of children's data requires both the child's parents or legal guardian and a juvenile and family court judge.[61] Dr. Boshe Patricia discusses this in her contribution on "A Thought on Child's Best Interest in Data Protection" in the KAS Law Talk Publication "Regulating Personal Data Protection and Cybersecurity.[62] She argues that the court has a unique position in assessing the processing of child consent, considering their age, maturity, and environment. Judges must balance the parental rights and responsibilities while also acknowledging the children's evolving autonomy and privacy based on the child's best interest. Beyond this, the judiciary can enforce principles by holding data controllers and processors accountable for failure to obtain verifiable parental consent.[63] They can also address corporate non-compliance regarding targeted advertising that violates domestic law and international conventions. Through this judicial mechanism, judges may order several reliefs such as injunction, mandate compliance from corporate entities and parents, or award damages caused to the child.[64]

Currently, Cambodia might not be able to use this component yet, as we don't have a family court, nor are court decisions publicized,[65] and judicial oversight might also lead to other challenges in enforcing personal data protection against large international social media companies.[66] However, it is crucial for the civil division to hear cases involving family and children's rights that have now extended digitally.

# VI. Conclusion

Ultimately, this brief addresses the remaining inadequacies for the upcoming PDPL to distinguish between children and adolescents as vulnerable data subjects, upholding children's best interests. As it is crucial for Cambodia moving forward to protect Children's personal data on Social media platforms for effective parental oversight and corporate compliance.

[56] Civil Code of Cambodia, Article 21, 22.
[57] United Nations Convention on the Rights of the Child, adopted November 20, 1989, G.A. Res. 44/25, 1577 U.N.T.S. 3 (entered into force September 2, 1990), Article 3, 16, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.
[58] Legal Information Institute, "best interests of the child," WEX, Cornell Law School, n.d., https://www.law.cornell.edu/wex/best_interests_(of_the_child.
[59] Boshe, "Child's Best Interest," 95.
[60] Moritz Hennemann and Patricia Boshe, "Data Protection Laws in Northern Africa: Regulatory Approaches, Key Principles, Selected Documents" (Konrad-Adenauer-Stiftung, September 2022), 3, https://www.kas.de/documents/265308/22468903/230406_DataProtectionLawsNorthernAfrica_KAS_Web.pdf/.
[61] DLA Piper, "Tennessee," DLA Piper Data Protection Laws of the World, last modified February 6, 2025, https://www.dlapiperdataprotection.com/index.html?t=law&c=TN; CMS, "Algeria," in CMS Expert Guide to Data Protection and Cyber Security Laws, last updated February 9, 2025, https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria.
[62] Kong and Honnet, Regulating Personal Data.
[63] Electronic Privacy Information Center (EPIC), "Children's Privacy - Data Protection," EPIC, last modified June 12, 2025, https://epic.org/issues/data-protection/childrens-privacy/.
[64] Tilleke & Gibbins, "Regional Guide to Cybersecurity and Data Protection in Mainland Southeast Asia" (PDF, Tilleke & Gibbins, July 2020), 10, https://www.tilleke.com/wp-content/uploads/2020/07/Tilleke-Regional-Guide-to-Cybersecurity-and-Data-Protection-in-Mainland-Southeast-Asia.pdf.
[66]"Has the Battle Just Begun for Collective Action against Big Tech Companies?" Conflict of Laws.net, January 11, 2022. https://conflictoflaws.net/2022/has-the-battle-just-begun-for-collective-action-against-big-tech-companies/.

This can be further achieved through implementing a tiered age threshold of digital consent that provides special protection for both groups, including an exception when appropriate, drawing from international practice outlined in the LGPD and POIPA models. Despite the current judicial limitations, Cambodia's courts could benefit in the foreseeable future, particularly in cases such as emancipation that have also not been addressed, potentially overriding traditional parental consent.

# Safeguarding Privacy, Enabling Access: Regulating Encryption in Cambodia's Digital Era


## MEAN Sopordaliss

[Development Cooperation Officer at Council for the Development of Cambodia]- KASFLY 2023

She holds bachelor's degree in Law and International Economics. She was a KASFLY 2023 fellow and has gained valuable legal experience working at Davies SM Attorneys-at-law, in addition to serving as a political intern at the US Embassy. Sopordaliss has been awarded several prestigious exchange scholarships, including as an exchange student in the JENESYS program in 2019, at Nanyang Technological University in 2023, and at St. Norbert College in the USA in Spring 2024 under the Global UGRAD Exchange Program.


# I. Introduction

Cyberthreats continued to escalate, with 72% of the Global Security Outlook survey reporting a rise in cyber risks, with a rise in both frequency and sophistication.[1] At the core of these issues is cryptography, which is a method of securing information that has existed for centuries and is now crucial to data protection in today's digital world.[2] By definition, cryptography is the discipline that embodies principles, means and methods for providing information security, including confidentiality, data integrity and authenticity.[3] "Encryption" is the principal application of cryptography; it transforms usable data into an unreadable form.[4] In its simplest form, encryption scrambles a message or document so that only the intended recipients can view or access the contents.[5]

As people become more reliant on technology, encryption is essential for protecting data integrity and individual privacy. Encrypted communications are used by governments, businesses, and individuals to protect sensitive data systems from unwanted access and to guarantee the privacy of digital communications. However, there are also complex legal and regulatory issues associated with this widespread reliance on

[1] World Economic Forum. Global Cybersecurity Outlook 2025. Geneva: World Economic Forum, 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.
[2] Dooley, John F. 2016. History of Cryptography and Cryptanalysis - History of Computing: Introduction - A revolutionary Cipher. Springer International Publishing AG, part of Springer Nature. https://doi.org/10.1007/978-3-319-90443-6_1.
[3] National Institute of Standards and Technology. "Cryptography." Computer Security Resource Center Glossary. Accessed May 16, 2025. https://csrc.nist.gov/glossary/term/cryptography.
[4] Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption (San Francisco: No Starch Press, 2018), 1, http://www.mypetskunk.com/uploads/1/0/6/1/106105481/seriouscrytography_ebook.pdf.
[5] Tricia E. Black, Note, Taking Account of the World As It Will Be: The Shifting Course of U.S. Encryption Policy, 53 FED. COMM. L.J. 289, 292 (2001).

encryption.[6] While encryption tools enhance privacy and reinforce secure digital communications, they can also hamper legitimate law enforcement efforts.[7]

As of 2025, Cambodia has not enacted a comprehensive legal framework that addresses encryption in particular. Instead, national legislation and various sectoral regulations have certain provisions related to data privacy and information security. The regulation of data encryption sits at the intersection of two fundamental legal domains, the right to privacy, including protection of personal data and cybersecurity, which encompasses national and digital security concerns.[8] Therefore, it is necessary to carefully examine how encryption serves both individual rights and the public interest in order to develop a coherent and balanced regulatory approach.

The legal issue surrounding encryption in Cambodia centres on the conditions under which authorities may access encrypted data, and what legal protections need to be put in place to protect individuals' privacy. Under Article 40 of the Constitution, individuals are guaranteed the right to privacy, including the confidentiality of correspondence, communications and personal information. This constitutional guarantee is further enshrined in Sub-Decree 252 on the Management, use and protection of personal identification data, which identifies subjects of personal data,[9] and in sectoral laws including the E-Commerce Law (2019) and on technical guidance on encryption in the banking sector that are not legally binding beyond the financial sector.

This legal gap presents a conflict between two opposing needs: the protection of individual privacy on one hand, and the state's responsibility to investigate and prevent crime on the other. These two objectives cannot be fully achieved simultaneously. Thus, the legal challenge is determining whether access to encrypted data is feasible without undermining the constitutional right to privacy, to guarantee a legally justified access to encrypted data under a clear legal framework with judicial and legislative safeguards.

# II. The Encryption Deilemma in Cambodia's Emerging Data Privacy Framework: From Constitutional Guarantee to Regulatory Silence:

There is currently no specific and thorough legal framework governing encryption or cryptographic technologies in Cambodia. Rather, the existing approach is distributed across constitutional provisions, procedural codes, and sector-specific regulations. These instruments mention encryption-related elements only in passing, often without substantive technical or enforcement guidance. The table below summarizes the legal touchpoints across relevant Cambodian laws and regulations:

[6] Nathan Saper, "International Cryptography Regulation and the Global Information Economy," Northwestern Journal of Technology and Intellectual Property 11, no. 7 (2013): 677.[2] Dooley, John F. 2016. History of Cryptography and Cryptanalysis - History of Computing: Introduction - A revolutionary Cipher. Springer International Publishing AG, part of Springer Nature. https://doi.org/10.1007/978-3-319-90443-6_1.
[7] Amit Singh and Praveen Singh Chauhan, "Breaking the Code: Legal Responses to Encryption in Cybersecurity Threat Scenarios," International Journal of Law, Justice and Jurisprudence 4, no. 2 (2024): 281.
[8] Swire, Peter, and Kenesa Ahmad. 2012. "Encryption and Globalization." The Columbia Science & Technology Law Review XIII: 416–81.
[9] Sub-Decree No. 252 on the Management, Use, and Protection of Personal Identification Data. Royal Government of Cambodia, No. 252 ANRK.BK enacted on 22 December 2021 ("Sub-decree No. 252"), Article 3

| Legal Instrument | Relevant Provision | Coverage of Encryption | Limitations |
|---|---|---|---|
| **General Law** | | | |
| **Constitution** | General right to privacy in correspondence (e.g., mail, telephone)[10] | Implicit only; no technical or regulatory elaboration | No implementing legislation; broadly stated and vague |
| **Criminal Procedure Code** | Judicial authority to intercept telecommunications[11] | Permits interception, including internet messages; no clarity on encrypted data | Lacks procedural safeguards or technical standards for encrypted communications |
| **Sub-Decree 252** | Guarantee the safety of personal data with the highest technical safety standards[12] | No direct regulation of encryption | Focused only on MOI-held ID data |
| **Sectoral Law** | | | |
| **E-Commerce Law (2019)** | Obligation to protect stored electronic data; Art. 43 restricts use of encrypted electronic data or devices related to offenses[13] | Mentions encryption implicitly in law enforcement context | Does not specify encryption standards or mechanisms for lawful access |
| **Prakas on Credit Reporting (NBC)** | Data protection through access control and user consent[14] | Addresses access restrictions; refers to security, not specific cryptographic methods | Limited to the financial sector; lacks broader applicability |
| **Technology Risk Management Guidelines (2019)** | Requires encryption safeguards, key management, and auditing in banking[15] | Contains specific guidance on cryptographic controls based on risk | Applies only to regulated financial entities; requires alignment with broader national laws, which remain underdeveloped |

The Constitution guarantees a general right to privacy in broad terms. It does not offer interpretations or procedural elaboration on the regulation of encryption or digital communication privacy. The Criminal Procedure Code empowers investigating judges to intercept communications, including online messages, but it does not address encrypted data or define limits to ensure proportionality and necessity.

Sub-Decree No. 252 on the management, use and protection of personal identification data articulates more detailed regulations regarding the protection of personal data, which specifically govern personal ID data managed and owned by the Ministry of Interior (**MOI**). However, the Sub-Decree does not directly address or regulate encryption practices, nor does it provide technical or procedural guidelines for safeguarding data through cryptographic methods. This limits its effectiveness in a digital environment where encryption is an essential tool for securing sensitive information.

The E-commerce law (2019) states the obligations to protect data, but it does not mention any specific mechanisms that should be used; however, it mentions some elements related to encryption, particularly in Article 43, which is to provide information to authorities that are related to offense.

[10] Article 40, The Constitution of Cambodia
[11] Cambodia Criminal Procedure Code, Royal Kram NS/KRM/1109/022, promulgated on October 12, 2009 ("Criminal Procedure Code") Article 172,
[12] Sub-Decree No. 252, Article 15
[13] Law on E-Commerce, Royal Kram NS/RKM/1119/016, promulgated on November 02, 2019 ("E-Commerce Law") Article 32 & Article 439
[14] National Bank of Cambodia, Prakas on Credit Reporting No. B7-020-352 BRK, June 26, 2020, Article 11
[15] National Bank of Cambodia, Technology Risk Management Guideline, p13, July 2019

However, questions regarding compliance and enforcement are still present because this regulation does not specify encryption systems or clear technological requirements.

For more detailed guidance, it is found in the banking sector, in which the National Bank of Cambodia (**NBC**) has issued the Prakas on Credit Reporting and Technology Risk Management Guidelines. These frameworks touch upon cryptographic controls, secure key management, and proportional use of encryption based on risk assessments. Nevertheless, their scope is applied to financial institutions and depends on national laws that have yet to be fully articulated.

In addition to the above, the IDPoor Department of the Cambodian Ministry of Planning has adopted a Data Protection Policy as a guiding framework for the Ministry, but also and its implementing partners in the absence of a comprehensive data protection law and an independent Data Protection Authority in Cambodia.[16]

# III. Benchmarking Cambodia's Encryption Rengulation: Lessons From International Models

Cambodia has yet to articulate a separate legislation or regulation on encryption technologies, whether in the context of personal data protection or within the broader cybersecurity framework. The legal dilemma about encryption typically revolves around whether encryption should be regulated. However, it is worth knowing that encryption is already the subject of existing laws and regulations around the world.[17] In the absence of a comprehensive national framework on encryption, this section undertakes a Comparative legal research methodology, drawing insights from international models exploring how other countries have addressed the legal balance between encryption, privacy and lawful access to benchmark Cambodia's current legal gap.

To address this legislative gap, this section benchmarks Cambodia against jurisdictions including the European Union, the United States, Canada and Australia. These frameworks are not introduced for direct transplantation of the legal models but rather for the normative guidance in structuring procedures and institutional safeguards. These legal models have been chosen for their normative influence on international data governance standards, their evolving legal debates on encryption access, and their diverse regulatory tools ranging from data protection instruments to investigatory access regimes.[18]

Legal responses to encryption vary widely depending on national priorities, constitutional frameworks and national concerns.[19] Although Cambodia differs in institutional capacity, legal traditions and level of digital infrastructure, its experiences offer important insights from a benchmarking perspective. Rather than treating these jurisdictions as direct comparators, this analysis uses them as normative benchmarks to identify legal, procedural, and institutional elements that promote a fair and accountable approach to encryption regulation. These insights may help to provide an

[16] Department of Identification of Poor Households. 2022. "Data Protection Policy – Department of Identification of Poor Households." October 14, 2022. https://idpoor.gov.kh/en/data-protection-policy/. Accessed on 12 June, 2025.
[17] Dizon and Upson, 2021."Laws of Encryption: An Emerging Legal Framework." Computer Law and Security Review Volume 43. November 2021. https://doi.org/10.1016/j.clsr.2021.105635 .
[18] Amit Singh and Praveen Singh Chauhan, "Breaking the Code: Legal Responses to Encryption in Cybersecurity Threat Scenarios," International Journal of Law, Justice and Jurisprudence 4, no. 2 (2024): 281-285.
[19] Ibid.

informative approach to encryption regulation with Cambodia's constitutional protection and the evolving digital governance regime.

## 1. Right to Privacy by Design and Legal Integration of Encryption

Encryption is widely acknowledged as a technical and legal safeguard for personal data. In the European Union, this principle is legally enshrined in the General Data Protection Regulation (**GDPR**), particularly under Article 25, which articulates data protection by design and default, requiring organizations to implement adequate encryption measures to protect personal data. Hence, the GDPR focused on both encouraging the use of encryption and encouraging cooperation between tech companies and law enforcement within the legal framework.[20] Instead of mandatory decryption, the EU's framework focuses more on structured cooperation mechanisms between service providers and law enforcement.[21]

Similarly, Canada's Personal Information Protection and Electronic Documents Act (**PIPEDA**) requires organizations to implement safeguards, including encryption, to protect personal data.[22] The PIPEDA applies to private-sector organizations across Canada that collect, use, or disclose personal information in the course of a commercial activity.[23] Canada's encryption law model is notable for its risk-based and consent-driven approach. While encryption is not mandated outright, failure to adopt reasonable security measures, including encryption for personal data protection, could lead to liability. Businesses are responsible for protecting all personal information, regardless of how it is stored, against loss, theft, unauthorized access, disclosure, copying, use or modification.[24] To fulfill that responsibility, it mentioned encryption as an example of up-to-date technological tools to protect personal data.[25] Likewise, the US follows a more sector-specific approach, such as the Health Insurance Portability and Accountability Act (**HIPAA**), which requires all healthcare providers, insurers, and other organizations handling patient data to encrypt any electronic protected health information (**ePHI**) they generate, receive, store or send.[26] Moreover, the Sarbanes-Oxley Act compels public corporations and accounting firms to protect their financial data, and the Gramm-Leach-Biley Act also requires financial institutions to put in place appropriate measures to safeguard consumer data, such as encryption.[27]

The GDPR shows how encryption can be used to protect individuals' rights and allow the government limited access in necessary circumstances. Cambodia's Constitution, under Article 40, guarantees the right to privacy, yet this constitutional guarantee has yet to be effectively operationalized in the digital domain. As of 2025, Cambodia has yet to have a comprehensive data protection law that would operationalize this constitutional right, particularly regarding imposing mandatory encryption requirements or setting out standardized technical safeguards. While Cambodia has enacted Sub-decree No. 252 on the management, use and protection of personal identification data (2021) and the IDPoor Data Protection Policy,[28] which governs the use of personal and household data collected through the country's poverty identification program, they are yet to specify the mechanism of data protection or technical encryption standards. Encryption is mentioned in Technology Risk

[20] Singh & Chauhan (2024) International Journal of Law, Justice and Jurisprudence; 4(2): 281-285. https://www.lawjournal.info/article/148/4-2-42-323.pdf
[21] Maria Koomen, "The Encryption Debate in the European Union," Carnegie Endowment for International Peace, May 30, 2019, https://carnegieendowment.org/posts/2019/05/the-encryption-debate-in-the-european-union?lang=en.
[22] Section 4.7.3, Canada Personal Information Protection and Electronic Documents Act. S.C. 2000, c. 5.
[23] Office of the Privacy Commissioner of Canada, "PIPEDA in Brief," Office of the Privacy Commissioner of Canada, last modified October 2022, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.
[24] Ibid.
[25] Ibid.
[26] National Research Council (US) Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, Globalization, Biosecurity, and the Future of the Life Sciences (Washington, DC: National Academies Press, 2006), https://www.ncbi.nlm.nih.gov/books/NBK500019/.
[27] Johnson, Data Encryption Laws: A Comprehensive Guide to Compliance, SecureITWorld, https://www.secureitworld.com/article/data-encryption-laws-a-comprehensive-guide-to-compliance/
[28] Department of Identification of Poor Households. 2022. "Data Protection Policy – Department of Identification of Poor Households." October 14, 2022. https://idpoor.gov.kh/en/data-protection-policy/. Accessed on 12 June, 2025.

Management in NBC guidelines, showing that Cambodia recognized encryption tools as a measure for safeguarding sensitive information based on risk assessment, yet this is only articulated for guiding the finance sector. The forthcoming data protection law, currently under government drafting,[29] presents an important opportunity to incorporate encryption as a legal and technical safeguard especially mandating encryption obligations for institutions that handle sensitive categories of information which may include public bodies managing national ID databases, telecom operators handling communication metadata, financial institutions processing payment information, and healthcare providers managing medical records.

## 2. Lawful Access and Procedural Safeguards

One of the central tensions in encryption regulation arises when governments seek lawful access to encrypted communications for criminal investigations. Although encryption plays a fundamental role in protecting the confidentiality, integrity, and authenticity of data, it also poses challenges to law enforcement when it is used to conceal criminal activity. The dilemma over encryption and law enforcement arose out of the case of *Apple v. FBI* when the US government attempted to compel Apple to unlock an encrypted phone, prompting debates over constitutional rights and commercial security obligations.[30] The debate over encryption continues and comes with several proposed legislative measures, including the Compliance with Court Order Act and EARN IT Act, which mandates the requirement of companies to provide access to encrypted data under certain circumstances.[31] Meanwhile, in Australia, the Assistance and Access Act 2018, also known as the Australian Data Encryption Laws, grants law enforcement the authority to request technical assistance from service providers to access encrypted information. Australia's Assistance and Access Act supports encryption as a cybersecurity tool but allows law enforcement to request access to encrypted data under strict legal conditions. The Act supports encryption as a cybersecurity tool but permits law enforcement to request access to encrypted information under strict legal conditions. It includes safeguards measurements such as judicial approval, oversight by independent bodies, and proportionality assessments.[32]

The legal framework relevant to access to lawful access to communications is addressed under Article 172 of the Code of Criminal Procedure, which authorises the investigating judge to order the interception and records of telecommunications, which also permits to request of technical assistance from qualified public institutions or specialist civil servants to carry out such recordings. Complementing this, the E-Commerce Law contains provisions discouraging the use of encryption to conceal information related to criminal offenses.[33] These frameworks already provide foundations governing criminal investigations. However, it is unclear on the subject of encrypted communications, the legal conditions under which decryption may be compelled and the procedural safeguards needed in the era of end-to-end encryption.

A clear and enforceable legislative framework that specifies when and how law enforcement can access encrypted data would be beneficial for Cambodia as encryption becomes more and more integrated in daily communications. Examples from Australia's Assistance and Access Act 2018 demonstrate insights for Cambodia to define encryption-related lawful access clearly, including lawful access to encrypted data only under exceptional circumstances, with judicial authorization,

[29] "Data Protection Laws in Cambodia - Data Protection Laws of the World." n.d. https://www.dlapiperdataprotection.com/index.html?t=law&c=KH
[30] Electronic Privacy Information Center, "Apple v. FBI" March 10, 2014, https://epic.org/documents/apple-v-fbi-2/.
[31] Amit Singh and Praveen Singh Chauhan, "Breaking the Code: Legal Responses to Encryption in Cybersecurity Threat Scenarios," International Journal of Law, Justice and Jurisprudence 4, no. 2 (2024): 283.
[32] Ibid.
[33] Article 43, E-Commerce Law Cambodia.
[34] Australian Government, Department of Home Affairs, The Assistance and Access Act 2018. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption.

# IV. Conclusion

In conclusion, the absence of a dedicated legal framework on encryption in Cambodia presents a significant regulatory gap. While sectoral laws and guidelines make reference to the establishment of data protection mechanisms, these provisions lack clarity and enforceable standards specific to encryption technologies. Accordingly, Cambodia may consider prioritizing the development of a comprehensive encryption regulation that clearly stipulates the obligations of the private sector and oversight of lawful access mechanisms to align with international best practices and to meet the goals in its Digital Economy and Society Framework. Such regulations would benefit Cambodia in a better position to navigate the challenges of its digital revolution.

# Biometric Data: Balancing Digital Innovation with Privacy Rights in Cambodia


## LIM Yseang

[Senior law student at ELBBL of RULE]

She is currently working as a legal intern at a law firm. She participated in the 21st Willem C. Vis East International Commercial Arbitration Moot and received the David Hunter Award for Best Written Memorandum for Claimants – Honorable Mentions among 144 participating teams. She has also participated as a mooter in the Foreign Direct Investment International Arbitration Moot and received "Best Teams 2024.


# I. Introduction

Biometric data has become a crucial component of digital transformation across the world.[1] Biometric data refers to unique biological characteristics of a person, such as fingerprints, facial recognition, and iris scans, used for authentication and identification.[2] In Cambodia, the use of biometric technologies in both public and private sectors improves identity verification's speed and accuracy.[3] However, biometric data is inherently more sensitive than traditional personal data due to its permanent link to an individual's physical characteristics.[4] Biometric data cannot be altered once it has been compromised, unlike passwords; breaches are irreversible and present a far higher and more persistent risk to users' security and privacy.[5]

In addition to technical risks, the lack of a comprehensive legal framework in Cambodia makes people more worried about the misuse of biometric data. As there are no clear rules governing how biometric data should be protected. Biometric data can be exploited for mass surveillance, identity theft, and other abuses that undermine public trust in digital systems.[6]

In this regard, this brief examines whether the use of

[1] Monty Greg, "Biometric Technology: The New Face of Security and Personal Identification," Cultivated Knowledge, 2025. https://cultivatedknowledge.com/technology/biometric-technology-the-new-face-of-security-and-personal-identification/.
[2] General Data Protection Regulation (GDPR), Art.4 (14).
[3] Bhosale Snehal, et.al. "Legal Challenges of Biometric Systems in Public Spaces: Surveillance vs. Privacy," Biometric Technology Today, vol. 2024, no. 8, 2024: p.54
[4] Bhosale et al. "Legal Challenges of Biometric Systems in Public Spaces: Surveillance vs. Privacy," op. cit., p.54.
[5] Akinsuru Adedoyin, "Legal and Ethical Implications of Biometric Data," ResearchGate, February 2025. https://www.researchgate.net/publication/388724072_Legal_and_Ethical_Implications_of_Biometric_Data_Usage_in_Modern_Governance.
[6] Ibid.

biometric data in Cambodia for surveillance purposes, in the absence of a comprehensive legal framework regulating its collection, processing, and storage, may constitute a violation of individuals' right to privacy as protected under Article 40 of the Cambodian Constitution and Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**).

By examining this legal problem, this brief aims to analyze Cambodia's legal framework by establishing the foundation for understanding the definition and categorization, processing, dispute resolution, protection, and retention of biometric data. Furthermore, identifying core challenges and drawing on international best practices from the EU's General Data Protection Regulation (**GDPR**), Singapore's Personal Data Protection Act (**PDPA**), and other international standards to develop a robust, rights-based framework for biometric data protection in Cambodia.

# II. The lack of legal protection of 'biometric data' under Cambodia's legal framework

Cambodia lacks a dedicated legal framework specifically addressing biometric data protection.[7] While data privacy provisions exist in Cambodian laws, they are still inadequate to address the needs of the rapidly growing digital economy.[8] Cambodia is currently drafting a Law on Personal Data Protection, which has yet to be enacted. As such, there is no binding legal provision that governs the collection and use of biometric data.

According to Article 40 of the Cambodian Constitution, the law recognizes citizens' right to privacy in broad terms, which provides that all Cambodian citizens have the right to privacy of residence, and to the secrecy of correspondence by mail, telegram *[...]*.[9] However, Cambodia does not yet have any specific legislation that elaborates on the meaning of this provision or provides any implementing measures for biometric data.[10] While this provision aligns with Article 17 of the ICCPR, it also does not explicitly address biometric data or provide implementing measures, leaving its application to sensitive data unclear and potentially insufficient to prevent arbitrary interference.[11] The growing integration of facial recognition technologies into public and commercial systems raises pressing legal questions.[12] The unregulated use of biometric surveillance in public spaces may lead to violations of the constitutional right to privacy and the potential criminalization of innocent individuals due to misidentification.[13] For example, the problem of deep fakes using artificial intelligence and biometric data together is concerning, as it can place an innocent individual at a crime scene.[14] Taking into account that biometric technologies cannot ensure full accuracy, there is always an implicit risk coming from incorrect identifications.[15] Such false positives can result in decisions affecting individual rights.[16] Moreover, Article 32 (1) of the Cambodian Law on E-Commerce stipulates that

[7] Kate Lucente, Lea Lurquin, eds. "Data Protection Laws of the World: Cambodia," DLA Piper, 2025, p.9. https://www.dlapiperdataprotection.com/guide.pdf?c=KH.
[8] Ibid.
[9] The Constitution of the Kingdom of Cambodia, 1993, Article 40.
[10] Tilleke & Gibbins," Regional Guide to Cybersecurity and Data Protection: in Mainland Southeast Asia," Cambodia, July 2024, p1.
[11] International Covenant on Civil and Political Rights (ICCPR), 23 March 1976, Article 17.
[12] Bhosale et al. "Legal Challenges of Biometric Systems in Public Spaces: Surveillance vs. Privacy", op. cit., p.56.
[13] Ibid.
[14] Qandeel. "Facial Recognition Technology: Regulations, Rights and the Rule of Law," Frontiers in Big Data 7, 2024.
[15] Christopher U EBELOGU et al. "Privacy Concerns in Biometrics," IEEE-SEM Volume 10, no. 7, July 2019: p.49.
[16] Federal Trade Commission, "FTC Warns About Misuses of Biometric Information That Harm Consumers," May 2023,https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

*"any person storing an electronic record of private information shall use all means to ensure that the information is reasonably and safely protected."* [17] However, this law does not explicitly define biometric data or categorize it as sensitive personal information. This omission presents a significant legal gap in both commercial and governmental digital systems. Therefore, without defining a clear term of biometric data and distinguishing this category of data, there is inadequate protection and potential violations of individuals' rights to privacy.[18]

Besides that, Article 305 of the Cambodian Criminal Code addresses the infringement of individual privacy; it does not specifically cover violations involving biometric data.[19] In cases where biometric data is stolen or misused, such as facial images being used to unlock smartphones or access personal accounts, the law currently lacks clear provisions for legal redress.[20] In this regard, Cambodian law does not currently provide explicit resolution mechanisms for criminal sanctions, and violations of rights concerning the unauthorized collection, use, or disclosure of biometric data.[21] Lastly, based on Sub-Decree No.252 on the Management, Use, and Protection of Personal Identification Data, the text includes general protections for personal data. Still, it lacks clear definitions and provisions concerning biometric data.[22] Without an explicit classification of biometric identifiers as sensitive data, the law does not adequately address their elevated risk profile.[23]

# III. Key Challenges in Biometric Data Governance

The growing use of biometric technologies in Cambodia has outpaced the development of legal safeguards, creating significant gaps in data governance. Without clear definitions and protections, biometric data remains vulnerable to misuse, privacy violations, and ethical concerns.[24] This section outlines six key challenges Cambodia should address, ranging from legal definitions and processing rules to ethical safeguards and data retention, to ensure that biometric data is managed responsibly and in line with international best practices.

## 1. The Child Threshold: Individuals Under 16 Years Old

Cambodian law currently contains no statutory definition of the term biometric data, including the Law on E-Commerce, which creates a gap in legal regulation and leaves it vulnerable to inconsistent protection.[25] Article 32 of the Law on E-Commerce imposes general data security obligations, requiring that any "personal information in electronic form" be safeguarded.[26] and even defines an "electronic signature" to include a "biometric signature".[27] However, the law does not define biometric data or classify it as sensitive, unlike other personal data, creating a significant regulatory gap

[17] Law on Electronic Commerce, No. NS/RKM?1119/017, November 2, 2019, Article 32(1).
[18] Kate Lucente, Lea Lurquin. "Data Protection Laws of the World," Cambodia, DLA Piper, 2025. https://www.dlapiperdataprotection.com/guide.pdf?c=KH.
[19] Cambodian Criminal Code, November 30, 2009, Article 305.
[20] Abigail Chiu Mei Lim, et.al "Biometric data landscape in Southeast Asia: Challenges and opportunities for effective regulation," Computer Law & Security Review: The International Journal of Technology Law and Practice volume 56, April 2025: p.2.
[21] Oeurn Mealtey. et.al. "Labor and Employment Disputes 2024," edited by Lexology Panoramic. Bangkok: Tilleke & Gibbins, 2024. https://www.tilleke.com/wp-content/uploads/2024/12/Tilleke-Labour-Employment-Disputes-2024-Cambodia.pdf.Tilleke & Gibbins+2.
[22] Sub-decree no. 252 on the management, usage, and security protection of personal data, December 22, 2021.
[23] Kate Lucente, Lea Lurquin, eds. "Data Protection Laws of the World: Cambodia," DLA Piper, 2025, p. 9. https://www.dlapiperdataprotection.com/guide.pdf?c=KH.
[24] Punia. et.al, "Ethical Considerations and Legal Frameworks for Biometric Surveillance Systems: The Intersection of AI, Soft Biometrics, and Human Surveillance," in Cryptology and Network Security with Machine Learning, volume 918, Singapore: Springer, 2024, https://link.springer.com/chapter/10.1007/978-981-97-0641-9_45.
[25] Kate Lucente, Lea Lurquin, eds. "Data Protection Laws of the World: Cambodia," DLA Piper, 2025, p. 9. https://www.dlapiperdataprotection.com/guide.pdf?c=KH.
[26] Law on Electronic Commerce, Article 32.
[27] Ibid.

and leading to uncertainty about how biometric identifiers should be treated and protected.[28] This ambiguity could allow misuse in areas like surveillance or digital identity systems, where biometric data is increasingly used.[29]

Biometric data that is processed to uniquely identify a person falls into the category of sensitive data because of its unique, permanent nature, which poses significant privacy and security risks if misused.[30] Under EU GDPR, biometric data is defined as technical data from physical or behavioral traits that uniquely identify a person.[31] and is treated as a special category requiring heightened protection.[32] The GDPR explicitly added biometric identifiers to the special category rules precisely because the threshold for identifying someone biometrically is higher than for ordinary personal data and thus poses greater risks.[33] Similarly, Singapore's PDPA has issued detailed guidance on biometric data, defining it (fingerprints, facial recognition, and iris) and highlighting strict consent and purpose limits.[34]

Thus, Cambodia should codify clear definitions and categories in its data law. Establishing a clear definition of biometric data along the lines of the GDPR definition and declaring it a special or sensitive category.[35] This would help the country match international standards, thereby enhancing regulatory certainty, boosting public confidence, and preventing confusion about what protections apply to biometric identifiers.[36]

## 2. Processing and Purpose Limitation of Biometric Data

Processing biometric data presents several significant problems, primarily due to its inherent sensitivity, permanence, and potential for misuse.[37] One of the foremost issues is privacy intrusion. Biometric systems often collect data without users fully understanding how it will be used, stored, or shared, raising concerns about consent and surveillance.[38] In practice, data collection and use largely follow broad mandates, including public interest and security, without explicit individual consent or purpose constraints.[39]

According to Articles 5(1)(b) and 6 of GDPR mandate that personal data must be collected only for explicit, legitimate purposes and processed lawfully, with sensitive processing (like biometric ID) allowed only under strict conditions such as explicit consent or necessity for vital interests.[40] While processing sensitive data can bring many positive effects, it poses a high risk of harming people and may impact human fundamental rights.[41] The rapid development of technology poses risks for the processing of sensitive data about a person's state of health, race, or ethnic background.[42] Additionally, Singapore's PDPA similarly requires organizations to notify individuals of collection purposes and generally to process data only for reasonable and consented purposes.[43] Therefore, Cambodia

[28] Kate Lucente, Lea Lurquin. "Data Protection Laws of the World: Cambodia," DLA Piper, 2025, op. cit., p.9.
[29] Office of the United Nations High Commissioner for Human Rights (OHCHR), "Cambodia: Data, Surveillance Legislation 'Repressive, Must Not Be Implemented" UN Experts, 2022. (Accessed May 20, 2025) https://www.ohchr.org/en/press-releases/2022/02/cambodia-data-surveillance-legislation-repressive-must-not-be-implemented-un.
[30] Jasserand Catherine, "Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data," European Data Protection Law Review 2, no. 3 (2016): p.17.
[31] General Data Protection Regulation (GDPR), Art. 4 (14), Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1.
[32] GDPR, Art.9 (1).
[33] Ibid.
[34] Leck Andy, et.al. "Singapore: PDPC Publishes Guide on Responsible Use of Biometric Data in Security Applications." Global Compliance News, July 18, 2022. https://www.globalcompliancenews.com/category/asia-pacific/singapore/page/17/.
[35] Camelia. "GDPR Special Category Data: What It Is, How to Handle It, and Why It Matters." Sovy, April 6, 2023. https://www.sovy.com/blog/gdpr-special-category-data/.
[36] Council of Europe, "Modernization of the Data Protection," Convention 108, January 2022. (Accessed May 29 2025).
[37] Salome Chkhaidze, et.al, "Processing of Biometric and Genetic Data: European Standards," Tbilisi: Institute for Development of Freedom of Information, 2022, p.15. https://idfi.ge/en/processing_of_biometric_and_genetic_data.
[38] Willoughby Angus, "Biometric Surveillance and the Right to Privacy," IEEE Society on Social Implications of Technology, January 3, 2023.
[39] Kate Lucente, Lea Lurquin, "Data Protection Laws of the World: Cambodia," Data Protection Laws of the World, 2025.
[40] GDPR, Articles 5 (1)(b) & 6.
[41] Ketevan Kukava, "Processing of Biometric and Genetic Data," European Standards, 2022, https://www.academia.edu/73392040/Processing_of_Biometric_and_Genetic_data_European_Standards.
[42] Ibid.
[43] Personal Data Protection Commission, "Data Protection Obligations", PDPA, December 2024. https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act.

should incorporate clear legal bases and purpose limits in law and require that biometric data may only be collected for specified purposes and always with individuals' consent, as the GDPR and PDPA do.

## 3. Protection Principles

Cambodian law treats data protection as a general privacy obligation.[44] There is no requirement for data minimization or data protection, and no formal obligation for data controllers to appoint privacy officers. The E-Commerce Law requires only "reasonable security measures" for stored consumer data, with little guidance on specifics, and law enforcement can demand decrypted data at will.[45] Consent is not systematically required under existing Cambodian laws, meaning biometric data could be captured without individuals' informed approval. Taken together, Cambodia lacks robust obligations on limiting data collected and obtaining meaningful consent.

The GDPR explicitly mandates data minimization and privacy by design, requiring that only data necessary for the purpose be collected.[46] Controllers must implement technical or organizational safeguards and often conduct Data Protection Impact Assessments for high risk processing.[47] Similarly, Singapore's PDPA likewise imposes a protection obligation to make reasonable security arrangements and a consent obligation for collection and use; it even requires organizations to appoint a Data Protection Officer and publish a data protection policy.[48] Hence, Cambodian legislation should explicitly incorporate strong protection principles for biometrics by amending Sub-Decree No. 252 on the Management, Use, and Protection of Personal Identification Data to include data minimization, security measures, consent requirements, and accountability, which can provide immediate protections and align with international standards. This could include requiring consent before the collection of biometric features and mandatory security safeguards.[49] The law should also mandate accountability measures: by requiring certain organizations to conduct impact assessments before deploying biometric ID systems and to designate responsible officials.[50] Furthermore, having strict safeguards for biometric data in Cambodian law would ease concerns about privacy by limiting who can access the data, reducing misuse risks, and ensuring everything is transparent.[51]

## 4.Dispute Resolution Pathways

In the absence of a dedicated regulator or privacy tribunal, individuals must rely on general legal remedies. Articles 10 to 13 of the Cambodian Civil Code allow a person to seek a court injunction to stop unlawful processing and to order erasure of improperly held data.[52] In practice, individuals might petition the relevant ministry. For instance, the Ministry of Interior for national ID issues, or bring private lawsuits invoking the constitutional right to privacy.[53] However, these general remedies face significant challenges when applied to biometric data disputes, including a lack of specificity, judicial inefficiencies, and limited access to justice.

[44] Cambodia Counsel, "Data Privacy," Practical Advice on Doing Business in Cambodia. https://cambodiacounsel.com/data-privacy/.
[45] Kate Lucente et.al. "Data Protection Laws of the World: Cambodia," DLA Piper, 2025, op. cit., p.11.
[46] GDPR, Articles 5 & 25.
[47] GDPR, Article 5.
[48] Personal Data Protection Commission, "Data Protection Obligations," December 2024. https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act
[49] GDPR, Articles 5, 25 & 32.
[50] Sothie Keo, Sophearathna Ros, "Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia," in Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond, eds. Phallack Kong, Thomas Honnet (Phnom Penh, Cambodia: Konrad-Adenauer-Stiftung, Royal University of Law and Economics, and National University of Management, 2023), pp.50-51.
[51] United Nations Human Rights Office of the High Commissioner, "Cambodia: Data Surveillance Legislation Repressive, Must Not Be Implemented – UN Experts," OHCHR, February 2022, https://www.ohchr.org/en/press-releases/2022/02/cambodia-data-surveillance-legislation-repressive-must-not-be-implemented-un.
[52] Tilleke & Gibbins," Regional Guide to Cybersecurity and Data Protection in Mainland Southeast Asia," Cambodia, July 2024, p.2.
[53] Kimmarita Long. "Ministry of Interior working on privacy protections for data." The Phnom Penh Post, 27 January 2021. https://www.phnompenhpost.com/national/ministry-interior-working-privacy-protections-data.

The GDPR grants data subjects the right to lodge complaints with the data protection authority and to seek judicial remedies and damages if their privacy is violated.[54] Also, Singapore's PDPA allows individuals to file complaints with PDPC if organizations breach the law, mediate disputes between parties, and impose penalties on organizations as well.[55] Thus, Cambodia should incorporate clear data subject rights and complaint mechanisms into its framework by ensuring individuals' rights of access and erasure of their biometric data. A practical recommendation is to create an administrative complaint process where users can report misuse of their biometric data, and could also consider allowing civil penalties or damages for unauthorized biometric data disclosures to incentivize compliance. In short, an enforceable remedy system is needed so that people can hold data handlers accountable.

## 5.Ethical Concerns arising from biometric misuse

The deployment of biometric systems in Cambodia raises significant ethical concerns that likely violate privacy rights.[56] The collection of biometric data by government agencies can be seen as a form of mass surveillance if not properly regulated.[57] Without strong legal limits, biometric data could facilitate pervasive surveillance.[58] Cambodia's current framework lacks ethics review and human rights safeguards for high-risk applications of biometrics. Under GDPR, automated profiling that has significant legal or similar effects is tightly regulated.[59] Moreover, Singapore has its guidelines emphasize transparency and proportionality in biometric use.[60] Cambodia's current regime has few explicit limits on how biometrics may be used by the state.[61]In this respect, Cambodian regulators should explicitly address the ethics of biometric use and establish an oversight committee to review proposed surveillance uses of biometrics. For instance, notice when cameras or scanners are collecting biometric data. These measures will help ensure biometric technology is used ethically and with public trust.

## 6.Data Retention Policies

The data retention aspect of biometric systems poses an additional challenge to the right to privacy.[62] Currently, there is no clear legal rule on how long biometric or other personal data may be retained in Cambodia. The E-Commerce Law implicitly suggests disposing of consumer records when no longer needed, but enforcement is absent.[63] Without explicit retention limits, there is a risk that sensitive biometric templates could be stored far longer than necessary, increasing exposure from leaks.[64] Most privacy laws require that such data be deleted as soon as they are no longer needed for the purpose for which it was collected.[65] Under GDPR, it treats biometric data as a special category and imposes a storage limitation that the data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they were collected.[66] For example, the UK government's guidance for immigration records provides that fingerprints are normally kept for 10 to 15 years from enrollment and only longer if national security needs to justify it.[67]

[54] GDPR, Articles 77–82.
[55] Personal Data Commission Singapore. "Guide to Singapore's Personal Data Protection Act (PDPA)," Privacy Bee. https://business.privacybee.com/resource-center/guide-to-singapores-personal-data-protection-act-pdpa/.
[56] Katina Michael, "Biometric Surveillance and the Right to Privacy," IEEE Society on Social Implications of Technology, 2023.
[57] Ibid.
[58] Punia. et.al, "Ethical Considerations and Legal Frameworks for Biometric Surveillance Systems: The Intersection of AI, Soft Biometrics, and Human Surveillance." in Cryptology and Network Security with Machine Learning, 2024. op. cit. p.10.
[59] GDPR, Article 22.
[60] Teo Chee Hean, "Surveillance Cameras Can Keep Us Safer but Raise Privacy Concerns," Channel News Asia, November 17, 2022, https://www.channelnewsasia.com/singapore/surveillance-cameras-safe-raise-privacy-concerns-teo-chee-hean-htx-techx-summit-2608041.
[61] Kelliher Fiona. "Cambodian Facial Recognition Effort Raises Fears of Misuse." VOA News, June 15, 2023. https://www.voanews.com/a/cambodian-facial-recognition-effort-raises-fears-of-misuse-/7138262.html.
[62] Angus Willoughby, "Biometric Surveillance and the Right to Privacy," IEEE Technology and Society Magazine, 2017.
[63] Law on E-Commerce, Article 10.
[64] GDPR Advisor, "GDPR and Biometric Data: Privacy Implications and Regulatory Compliance," 2023. https://www.gdpr-advisor.com/gdpr-and-biometric-data-privacy-implications-and-regulatory-compliance/.
[65] GDPR, Article 17 and Recitals 65 & 66.
[66] GDPR, Article 5(1)(e).
[67] Gov UK. "Retention and Usage of Biometric Information." March 24, 2025. https://www.gov.uk/government/publications/biometric-information/retention-and-usage-of-biometric-information-accessible.

Moreover, California's CCPA gives individuals the right to deletion, and limits on the use of sensitive data under CPRA implicitly discourage indefinite retention.[68] In *S & Marper v. UK*, the European Court of Human Rights held that indefinite retention of biometric data, like DNA and fingerprints, from individuals not convicted of crime violates privacy rights.[69] Such data is highly sensitive, and retention must be proportionate and time-limited to protect privacy rights.[70] Therefore, Cambodian law or regulations should establish concrete retention limits for biometric data. By embedding retention constraints in the law, Cambodia can reduce the risk of unnecessary data align with global data protection practices.

# IV. Conclusion

Cambodia's increasing adoption of biometric technology, particularly in both the public and private sectors, presents both opportunities and challenges. While biometrics offer a secure and convenient method for verifying identity in digital transactions, the lack of a comprehensive legal framework specifically governing biometric data poses significant risks to data privacy and security. To address these shortcomings, Cambodia should introduce a comprehensive Biometric Data Protection Law that aligns with international standards, such as the EU GDPR and those of the US and Singapore. The law should define and recognize biometric data as a sensitive category and include specific guidelines on biometric data protection, as well as robust security measures and the establishment of a regulatory oversight body. By taking these steps, Cambodia can harness the benefits of biometric technology while safeguarding the privacy rights of its citizens and promoting trust in the digital age.

[68] Rob Bota, "California Consumer Privacy Act (CCPA)," March 2024.
[69] S. and Marper v. the United Kingdom, ECHR, 2008.
[70] Ibid.

# Enhancing Oversight on Cambodian Personal Data: Adequacy Decision On Cross-Border Data Transfers to the European Union

**SUN Neakputhkun**

[ Junior Associate at Sok Xing & Hwang]

With experience providing legal advice to both local and international clients, she focuses on corporate, commercial, labor and employment, and real estate transactions. She holds a Master's Degree in Private Law and a Bachelor's Degree in Law from Royal University of Law and Economics. She is particularly passionate about digital privacy, corporate law, labor and employment.

## I. Introduction

Cross-border trade in digital goods and services is increasingly reliant on seamless flows of personal data, particularly in industries such as targeted advertising and e-commerce. This reliance necessitates a balance between facilitating data flows for economic growth and maintaining high data protection standards. Thus, two elements are essential for achieving this goal: one, the establishment of an independent data protection supervisory authority, and two, the formation of a transparent and accountable framework for issuing decisions on cross-border data transfers. An adequacy decision is a formal determination to the recipient country that offers an adequate level of data protection, allowing for the transfer of personal data to that entity without additional safeguards. Without a clear principle of legitimate necessity and an adequacy standard, the enforcement of an adequacy decision could become inconsistent and ineffective. Legitimate necessity is a principle that guarantees personal data is processed only when essential and lawful. Meanwhile, adequacy standard requires the recipient country to provide protection equivalent to that of the sending country. These issues led many jurisdictions, particularly the European Union (**EU**) and

Thailand, to formalize these legal principles, issue adequacy decisions, and establish supervisory bodies.

The EU's General Data Protection Regulation (**GDPR**) is a prominent data protection regulation with the adoption of an adequacy decision mechanism, leading many countries to adopt similar approaches. In this context, Thailand became the first country in Asia that adopt a GDPR-based Personal Data Protection Law with some key local differences[1] and recently established an adequacy decision mechanism. By analyzing the approach from the EU with a more advanced data protection standard and Thailand's approach with a similar legal system to Cambodia, this could provide insights for Cambodia to consider a more adaptable framework for adequacy decisions.

As of 2023, Cambodia has deepened its trade relations with the EU, now its fourth-largest trade partner. However, Cambodia lacks a comprehensive data protection regime. While legislative efforts to draft a personal data protection law are underway,[2] existing privacy protection remains fragmented across constitutional provisions and various laws.[3] For Cambodia to gain regulatory independence and credibility as a trusted player in the global digital economy, it is crucial to establish foundational mechanisms to meet those ends. Accordingly, Cambodia must enhance its legal framework by establishing a national supervisory authority and developing adequate decision-making in the recipient country to safeguard the privacy rights of citizens and national interests.

# II. Closing the Gaps: Legal Challenges and Solutions for Data Transfers in Cambodia

Cambodia has scattered regulations related to individual privacy; various aspects of privacy protection are included in the Cambodian Constitution, Civil Code, Telecommunications Law, and E-Commerce Law. Nonetheless, Cambodian laws and regulations fail to address personal data transfer across borders. Therefore, Cambodia needs to close this regulatory gap by developing a more stringent legal framework and aligning with global data protection standards. This brief article will explore four critical issues: 1) Broad Interpretation of Legitimate Necessity; 2) Limitations of Adequacy Standards; 3) Accountability Challenges with National Supervisory Authority; 4) Checks and Balances of Adequacy Decision.

## 1. Broad Interpretation of Legitimate Necessity

An undefined concept of "legitimate necessity" allows divergent interpretations, and undermines consistent enforcement to issue a decision on personal data transfer. Generally, legitimate necessity is a core principle to assess the lawfulness of processing personal data. Stated another way, this concept indicates that personal data should be collected and processed unless it is necessary for the completion of a clearly defined purpose. For instance, in the case of *Bundeskartellamt v. Meta Platforms Inc.,* the Court of Justice of the European Union (**CJEU)** emphasized that the legal basis of

[1] DLA Piper. Thailand. In Data Protection Laws of the World, 2025 ed., 9. London: DLA Piper, 2025.
[2] Royal Government of Cambodia. Cambodia Digital Government Policy 2022–2035, prepared by Ministry of Post and Telecommunications (Phnom Penh, 2022), 39.
[3] Tilleke & Gibbins. Cybersecurity and Data Protection in Mainland Southeast Asia: 2024 Edition. Bangkok: Tilleke & Gibbins, 2024, 2.

"necessary for performance of contract" under Article 6(1)(b) of the must be strictly interpreted. In this case, Bundeskartellamt (Federal Cartel Office, Germany), accused Meta of abusing its dominant market position by excessively collecting and combining user data in Germany across its platforms and third-party websites without user consent. In fact, Meta aggregated user data across multiple platforms and third-party websites (namely, Facebook, Instagram, WhatsApp, Oculus, and Masquerade) into a single detailed user profile, despite the user not actively using some of those services. Meta then used that data to create personalized advertisements.[4] The CJEU ruled that such personalized advertisement is not considered necessary for the performance of the contract because the services can still be provided without personalization. Consequently, Meta cannot use the legal basis of necessity for performance to justify its data collection practices for personalized advertisement. This brings critical attention to provide a clear definition of legitimate necessity, particularly "necessary for performance of contract," to avoid exploitation from data holders with massive data collection and misuse of the data for their monetary benefits.

The EU approaches this issue under Article 6 of GDPR with additional guidelines to clarify the concept of necessity and necessary for the performance of a contract. GDPR mandates six principles for lawful processing personal data with at least one of the following applies: 1) given consent of data subject; 2) necessary for performance of contract with data subject; 3) necessary for compliance of the controller's legal obligation; 4) necessary for protection of data subject's vital interests; 5) necessary for a task in public interest or official authority; and 6) necessary for legitimate interests pursued by the controller or third party.[5] To refrain from broad interpretation, the European Data Protection Board (**EDPB**) provides further guidance on applicability for necessary for performance of a contract to process personal data in the context of online services. This guideline outlines the elements of lawful processing under Article 6(1)(b) of GDPR and the detailed concept of necessity and necessity for the performance of a contract. For applicability of this article, the processing must be objectively necessary for a purpose that is integral to the delivery of that contractual service to the data subject.[6] The guideline also lists down questions for the assessment of whether Article 6(1)(b) is applicable, including nature of service, exact rationale of the contract, essential elements of the contract, how the service is promoted or advertised to the data subject, etc.[7]

With this in mind, Thailand adopted Personal Data Protection Act (**PDPA**) in 2019 and mandates that cross-border data transfer is allowed only if the recipient country has adequate data protection standards as assessed by Personal Data Protection Committee (**PDPC**) except the following necessary conditions: 1) The transfer complies with Thailand's PDPA; 2) given consent of data subject; 3) necessary for performance of contract with data subject 4) compliance with a contract between data controller and other persons 5) prevent or suppress danger to data subject when data subject is incapable of giving the consent 6) substantial for public interest.[8] Nonetheless, Thailand's PDPA does not provide detailed criteria or a definition of what constitutes each principle for the lawful processing of personal data.

To ascertain lawful international data flows, Cambodia should approach this issue by incorporating

[4] Bundeskartellamt v. Meta Platforms Inc., Case C-252/21, ECLI:EU:C:2023:537, Court of Justice of the European Union, Grand Chamber, judgment of July 4, 2023.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art. 6.
[6] European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, version 2.0, October 8, 2019, 9.
[7] European Data Protection Board, Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, version 2.0, October 8, 2019, 10.
[8] Personal Data Protection Act B.E. 2562 (2019) (Thailand), sec. 28.

principles of legitimate necessity, particularly "necessary for performance of contract," into the draft personal data protection law. Then, policymakers should consider providing additional guidance on a clear concept of necessity, including necessary for the performance of the contract. A set of questions for data controllers could be an integral part of this guidance for law enforcers to make an assessment on the applicability of the necessary requirements for the performance of contracts. By doing so, this could alleviate the risks of inconsistent practices by relevant actors and prevent excessive data collection for other unnecessary purposes.

## 2. Limitations of Adequacy Standards

An adequacy standard generally refers to the requirement that the recipient country must essentially provide an equivalent to that of the sending country. When the country fulfills all conditions, an adequacy decision will be issued to such country. In 1980, Organization for Economic Co-operation and Development released one of the first international frameworks for personal data protection called "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Privacy".[9] This guideline acknowledged that transborder flows of personal data are sources of a major concern, but also emphasized the need to avoid creating unjustified barriers to data transfer flows. European countries realized that older regulatory tools were insufficient to handle emerging risks as technology evolved rapidly. The EU thereby adopted a more structured geographically-based approach to adequacy decisions that applied to third countries and international organizations.[10] As such, the mechanism of adequacy decision was then introduced.

Article 45 of GDPR tasks the European Commission with conducting assessments of whether third countries offer adequate protection for personal data transfers. If the European Commission issues an adequacy decision to a country, personal data can flow freely without the need for additional safeguards. The assessment for an adequate level of protection follows three criteria as below:

**1.** Rule of law, respect for human rights and fundamental freedoms, relevant legislation as well as effective and enforceable data subject rights and effective administrative and judicial redress;

**2.** Existence and effective function of one or more independent supervisory authorities; and

**3.** International commitments (i.e., conventions or instruments).[11]

To balance between discretion and transparency, the adoption of an adequacy decision involves a proposal from the Commission, an opinion of the European Data Protection Board, an approval from representatives of EU countries, and the adoption of the decision by the Commission.[12] Primarily, the Commission conducts an adequacy assessment of the country. If the Commission finds that it offers an adequate data protection standard, the Commission prepares a draft adequacy decision.[13] The draft decision is then submitted to EDPB for review and issues an advisory opinion analyzing strengths, weaknesses, and recommendations.[14] Then, the draft adequacy decision and EDPB's opinion are presented to a committee of representatives of all EU member states, and the committee votes to approve or reject the proposal. Upon the approval, the Commission formally

[9] Organization for Economic Co-operation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1980).
[10] Hiroshi Miyashita, "EU-Japan Mutual Adequacy Decision," The EU-Japan Relationship 3, no. 7 (2020): 1.
[11] GDPR, art. 45(2).
[12] European Commission, "Adequacy Decisions," last modified April 15, 2024, European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[13] GDPR, art. 45(1) and (2).
[14] GDPR, art. 70(1)(s).

adopts the adequacy decision. [15]

Similarly, PDPA requires for recipient country to have adequate data protection standards.[16] However, Thailand's PDPA does not clearly define what constitutes an "adequate standard". Because a loophole in the cross-border transfer requirement existed for a long period, some organizations opted to manage risks by engaging in offshore transfers without seeking approvals or exemptions.[17] Later in 2023, Thailand issued subordinate regulations to establish adequacy decision mechanism under the PDPC Notification on Cross-Border Transfers. To satisfy adequacy standard assessment, the requirements must be as follows:

**1.** The recipient country or international organization must have legal measures or mechanisms aligned with Thailand's PDPA. Those include obligations to data controllers to have security measures to protect data subjects with enforceable legal instruments in the case of breaches; and

**2.** The presence of an agency or organization entrusted with the duties and authority to enforce laws and regulations related to personal data protection.[18]

As of present, PDPC has yet to list a specific country as adequately known as a "whitelist".[19] The absence of a whitelist and a blank history of adequacy decisions to recipient countries in Thailand has forced business operators to bear with difficulties of evaluating the adequacy of their personal data protection measures themselves.[20]

Setting adequacy standards could be beneficial for Cambodia to align with global best practices of data transfers across borders. Cambodia could emulate this approach within its local context by integrating the adequacy data protection standard into the draft data protection law. The policymakers could then develop criteria and conditions for adequacy standards with additional guidelines to supplement what constitutes an adequate standard to facilitate enforcement by relevant authorities. The criteria should require that the recipient country has comprehensive legal measures for data protection, along with the existence of a national supervisory authority to enforce data protection law. This is, however, inevitably involved complex and costly process. Inputs from stakeholders and relevant parties are essential for the effective implementation of this approach.

## 3. Accountability Challenges with National Supervisory Authority

Private entities are not the only ones that may abuse or mishandle citizens' personal data. This brings an even more important question is how much personal data governments should collect, store, and process on their citizens and what kind of legal precautions should be taken to protect privacy.[21]

The EU places strong emphasis on the accountability of its authority. GDPR mandates that each EU member state must establish one or more independent supervisory authorities.[22] In this connection, the staff of supervisory authorities are bound by professional secrecy obligations, both during

[15] GDPR, art. 45.
[16] Personal Data Protection Act B.E. 2562 (2019) (Thailand), secs. 28–29.
[17] Asian Legal Business, Thailand: Choices Surrounding Personal Data Breach Notification, May 2024, 20.
[18] Tilleke & Gibbins, "Thailand Unveils Regulations for Cross-Border Personal Data Transfer," Tilleke & Gibbins, December 25, 2023, https://www.tilleke.com/insights/thailand-unveils-regulations-for-cross-border-personal-data-transfer/.
[19] Asian Legal Business, "Thailand: Choices Surrounding Personal Data Breach Notification," Asian Legal Business, May 2024, 20.
[20] Asian Legal Business, "Thailand: Choices Surrounding Personal Data Breach Notification," Asian Legal Business, May 2024, 21.
[21] H. Akın Ünver and Grace Kim, "Cross-Border Data Transfers and Data Localization," Centre for Economics and Foreign Policy Studies, 2016, 7, http://www.jstor.org/stable/resrep14047.
[22] GDPR, art. 51.

and after their term of office.[23] The GDPR itself does not impose explicit penalties for breaches of confidentiality. Instead, each member state must establish appropriate rules and sanctions under their national law.[24] This indicates the commitment to ensure accountability of the authority in case of a confidentiality breach while handling individual personal data.

In Thailand, PDPC holds the power to request documents or information related to data protection.[25] However, PDPA does not impose sanctions on this committee or its members for breaches of confidentiality. Administrative and liabilities only apply to breaches that occur by data controllers and data processors under PDPA. [26]

This regulatory gap could undermine public trust and fairness in data protection enforcement. While supervisory authorities require protection to operate effectively, there must also be a mechanism to hold such authorities accountable for mishandling personal data. Under Cambodian law, disciplinary sanctions must be imposed on violations by civil servants, including first-degree and second-degree violations. Those sanctions include reprimand, demotion, dismissal and such.[27] To demonstrate a strong commitment to proper handling of personal data by local authorities, Cambodia could incorporate professional secrecy and sanctions for breaches of confidentiality or misconduct by the authority under subordinate regulations (such as a Sub-Decree) that establish and govern this supervisory body. The sanctions on the data handlers may include reprimand, dismissal or other fines following the actual legal structure of the supervisory body.

## 4. Check and Balence Of Adequacy Decision

The absence of a redress mechanism raises concerns about fairness and transparency regarding the adoption of an adequacy decision. Without this mechanism, this leads to excessive power granted to an enforcement body. A recent case demonstrates the importance of legal recourse to this decision. In the case of *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (known as Schrems II) raised questions on the reliability of the Commission's adequacy decision regarding the United States.[28] The adequacy decision granted under the Privacy Shield framework was invalidated by the CJEU from the findings of the United States government's mass surveillance over EU citizens.[29] Without an appropriate grievance mechanism, the affected individual may refrain from legal remedies.

The EU provides a redress mechanism under GDPR to strike a balance between power and impartiality. CJEU has the authority to revoke adequacy decision granted by the Commission.[30] The invalidation of the Privacy Shield Framework by the CJEU serves as a remedy to put pressure on the United States to improve its data protection standards and regulations to meet EU standards and ensure the privacy rights of EU citizens. Moreover, an individual has the right to a judicial remedy against such a decision of a supervisory authority.[31] This provides an additional layer to safeguard fundamental rights to data protection.

On the contrary, Thailand does not provide a challenge mechanism for decisions made by the

[23] GDPR, art. 54(2)(b).
[24] GDPR, art, 90.
[25] Personal Data Protection Act B.E. 2562 (2019) (Thailand), secs. 70–90.
[26] Privacy Laws & Business, Thailand: Personal Data Protection Act B.E. 2562 (2019), accessed June 17, 2025, https://www.privacylaws.com/media/2994/thailand.pdf, 5.
[27] Law on Common Statute of Civil Servants, dated October 26, 1994, art. 40.
[28] Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, Court of Justice of the European Union, July 16, 2020.
[29] Edward W. McLaughlin, "Schrems's Slippery Slope: Strengthening Governance Mechanisms to Rehabilitate EU–U.S. Cross-Border Data Transfers After Schrems II," Fordham Law Review 90, no. 1 (2021): 232.
[30] Treaty on the Functioning of the European Union (TFEU), art. 263, signed February 7, 1992, entered into force November 1, 1993, Official Journal of the European Union, C 326, October 26, 2012.
[31] GDPR, art. 78.

Personal Data Protection Committee. PDPA only provides redress mechanisms against violations by data controllers and data processors.

Following the approach of the EU, a redress mechanism can strengthen the efficacy of a decision made by the Cambodian law enforcement body. Cambodia could grant individuals the right to appeal decisions under the draft data protection law. Additionally, there should be options for individuals to refer to either the local supervisory authority or the competent court. Due to digital illiteracy and the absence of specialized court division in Cambodia, appealing an adequacy decision to the court can be a frustrating process. Therefore, filing a complaint with a national supervisory body is a more practical approach. If the party is still not satisfied, there should be another option for individuals to file a complaint to governmental agencies, such as the Ministry of Post and Telecommunication, a central role in drafting personal data protection law. This solution serves as a reinforcement of fairness in the issuance of adequacy decisions.

# III. Conclusion

Cambodia's effort to deepen digital integration with international partners, especially with the EU, positions cross-border data transfers as a cornerstone of economic modernization. The ongoing draft personal data protection will become pivotal to align the country with international protection norms. As of now, Cambodia does not restrict international data flows. Moreover, Cambodia's commitment is to open cross-border data flows to align with global data protection standards and its digital government policies with the objective of facilitating secure and harmonized cross-border data flows. Cambodia faces the challenges of developing data protection, particularly in adopting a clear legal interpretation of legitimate necessity and adequacy standard for data transfers. Drawing from the international legal framework under the EU's GDPR and Thailand's PDPA, these recommendations require a complex process and significant resources. Nevertheless, they offer a practical pathway for Cambodia to enhance the protection of Cambodian citizens' personal data while also boosting competitiveness in the global digital economy. By adopting the recommendation, Cambodia can effectively strike a balance between privacy protection, economic growth and trust among international partners. This could also open an opportunity for Cambodia to obtain an adequacy decision from the EU without the requirement of additional safeguards in the future.

# Bridging the Gap: Toward a Legal Framework for the Right to Erasure in Cambodia's Digital Age

**TENG Solisa**

[Lawyer Assistant in Litigation]

She is fresh law undergraduate from the Royal University of Law and Economics and holds a bachelor's degree in Fashion Design and Business Innovation from Limkokwing University. Previously, she participated in various academic and leadership development programs, such as the NUS Enterprise Summer Program in Entrepreneurship, the International Youth Fellowship, and the UNITWIN Legislation Camp.

## I. Introduction

Personal data is a valuable asset for individuals, and all online activities create a digital footprint that others can track and exploit for different purposes.[1] Although Cambodia currently lacks a comprehensive data protection law, other frameworks recognize and uphold individuals' privacy rights.[2] Despite this, no laws had explicitly touched on the right to erasure,[3] which empower individuals to control and delete their personal data. The absence of this fundamental right in the current data protection shout-out highlights the need for a closer look at regulation such as the European Union's General Data Protection Regulation (**GDPR**), which is the gold standard for data protection law.[4]

The jurisdiction mandates that countries regulate personal data protection frameworks to safeguard collected personal data and grant individuals 'certain rights, including the right to erasure. However, this is not unconditional; there are instances where data needs to be retained for legal or public interest reasons.[5] Article 17 GDPR provides that data can be held if it is needed to maintain freedom of expression and information. Complying with the legal regulation, protecting public health, assisting with archiving or research, or making and defending legal claims.[6]

[1] "The Importance of Data Privacy in the Digital Age," Compliance Hub, October 20, 2023. https://www.compliancehub.wiki/digital-privacy-in-digital-age/.
[2] Cambodia Constitution, Articles 10&40; Cambodia Civil Code, Royal Kram No. NS/RKM/1207/030, Article 12; Law on Consumer Protection, Royal Kram No. NS/RKM/1119/016, Article 32; Law on Telecommunication, Royal Kram No. NS/RKM/1215/017, Article 65(b).
[3] (EU) 2016/679 of the European Parliament and of the Council, Official Journal of the European Union, L 119, May 4, 2016, Article 17.
[4] Sears, Emilie. "International Regulations and the GDPR-Effect." RadarFirst, 2021.
[5] Ben Wolford, "Right to Be Forgotten," GDPR.eu.
[6] GDPR, Article 17.

Likewise, this paper aims at the legal gray areas and enforcement challenges surrounding the right to erase, focusing on the Cambodian legal standard and capacity. This demonstrates the problems that come up as we try to balance privacy and freedom of speech when data owners do not know what their responsibilities are, while transferring data across borders is challenging. Observing the (**II**) Scope and Applicability Ambiguities on Third Party Controller. Analyzing the (**III**) Tension Between the Right to Erasure and Freedom of Expression and explore the (**IV**) challenges in Cross-Border Data Erasure.

# II. Scope and Applicability Ambiguities on Third Party Controller

Despite the goal for the Law on Personal Data Protection being "Beyond compliance, a strong legal framework for data protection acts as a cornerstone for trust, confidence, and security in the digital domain."[7] This required the need to be transparent on how to handle structural and operational issues, which poses a potential challenge. If an individual asks for the erasure of their data, there may be ambiguity regarding the efficacy of the request.

Under Article 17(2), GDPR states that when personal data has been made public, data controllers,[8] must notify other data controllers about a data subject's need to erase the data. In support of this right in the digital realm, the data controller that has disclosed personal data must take appropriate measures to notify other controllers processing the data and delete any links, copies, or replicates.[9] This procedure involves using accessible technology and resources to support the data subject's request for erasure.[10] Even with such effort, shortcomings remain on what this obligation includes, such as the meaning of public disclosure, how to notify third-party controllers, or what responsibilities apply to data stored in backup or archival systems. The *Proximus v. Gegevensbeschermingsautoriteit case (C-129/21)* shows that Proximus made public disclosures and that the data controller must take sensible steps to inform other data controllers, like third-party directory services and possibly search engines, about the erasure request and make sure they follow the GDPR.[11] Additionally, BCWipe, which has been trusted by the U.S. Department of Defense to securely wipe files and data remanence beyond forensic recovery, also has three main guides to follow, such as verifying the request by confirming the identity of the individual who requested it and then locating all the available data and deleting it using a reliable data-wiping method.[12]

From another angle, Peter Fleischer, Google's Global Privacy Counsel, suggests outlining three typical situations describing a right to be forgotten on the Internet.[13]

[7] Cambodia Investment Review, "EuroCham Cambodia Continues Development of Data Protection Laws; Experts Highlight Importance of Aligning with ASEAN Standards," Cambodia Investment Review, 2024,. https://cambodiainvestmentreview.com/2024/02/05/eurocham-cambodia-continues-development-of-data-protection-laws-experts-highlight-importance-of-aligning-with-asean-standards/.
[8] European Commission, "What Is a Data Controller or Data Processor?" European Commission,.
[9] GDPR, Recitals 66.
[10] Ibid.
[11] Court of Justice of the European Union, Proximus SA v Gegevensbeschermingsautoriteit (GBA), Case C-129/21, judgment of October 5, 2023, EUR-Lex,.
[12] Hannaleena Pojanluoma, "How the Right to Erasure Is Applied Under GDPR: Complete Guide for Organizational Compliance," Jetico Blog, February 25, 2025, https://jetico.com/blog/how-right-erasure-applied-under-gdpr-complete-guide-organizational-compliance/#best.
[13] Michael L. Rustad and Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow," Harvard Journal of Law & Technology, March 22, 2015, 389, vol.28.

| Degree of Deletion | Description | Examples |
|---|---|---|
| First Degree of Deletion | Data subject's own postings and pictures online. | Data subject posts embarrassing pictures of himself on Facebook and seeks to erase them. |
| Second Degree of Deletion | Data subject posts content that a third party copies and reposts on the third party's own site. | Data subject posts on Twitter, and third-party retweets it on her own site. Data subject seeks removal of retweet. |
| Third Degree of Deletion | Third party posts data not created by the data subject but that is about the data subject. | Third party posts picture of or data about data subject on Facebook. Data subject requests removal of posting. |

**Table on Three Degrees of Deletion from Peter Fleischer**

This table touches on common scenarios and different types of deletion that should also be addressed to provide easy management. While the first degree is straightforward to solve, the second and third degrees might be challenging. The most viable solution for second-degree deletion is a user-driven approach, where the data subject finds and reports reposted or tagged content. Platforms could assist this process through privacy mechanisms. Such an approach provides an effective method for safeguarding personal data in complex internet environments.[14] As for the third degree, filing a legal complaint would be preferred.[15]

Here in Cambodia, it is recommended to have additional prakas that clearly define the responsibilities of third-party data controllers to ensure effective implementation of the right to erasure when personal data has been made public. Drawing from the EU GDPR and the Proximus case, it should define what constitutes public disclosure and establishes clear, accessible channels for data subjects to file such requests. Besides, incorporating Peter Fleischer's "three degrees of deletion" or a similar approach can further enhance practical enforcement. As digital data expands, Cambodia will need to establish legal mechanisms and approaches to address not just the initial controller but also the whole chain of data interactions. With the right to erasure, the data controllers need to have clear data management practices, set up strong consent processes, and create systems for sharing and coordinating erasure requests with everyone involved in handling and sharing data.

[14] Ibid.
[15] Ibid.

# III. Tension Between the Right to Erasure and Freedom of Expression

An apparent issue arose regarding the application of this right between the right to erasure and the right to freedom of expression and press.[16] In the Constitution of Cambodia, there are two basic rights that are relevant to the conflict in this situation. Article 40 of the Constitution of Cambodia, right to privacy, could provide a legal foundation for a future "right to erasure" like the one that is available under European data protection laws.[17] Although Article 41 of the Constitution of Cambodia, right to freedom of expression and the press, guarantees freedom of expression and the press, it must not infringe on others' rights, harm societal traditions, or violate public order and national security.[18] While each of these rights appears clear when considered individually, tensions may arise when they intersect once the right to erasure is adopted. For instance, one person may exercise their right to freedom of expression by sharing information, while another may seek to have that same information removed or concealed.[19] This conflict becomes even more complex in the digital era, where information is no longer stored solely on paper but is widely disseminated and preserved online.[20] As technology advances, balancing the two rights will require more nuanced legal and ethical considerations.

Although having a strong personal data protection right, the EU also recognizes the right to expression as a fundamental right, which is a right that allows *"freedom to hold opinions and to receive and impart information and ideas"*,[21] and the Google Spain case was the first to highlight the core tension between these rights.[22] The Court ruled to safeguard individuals from negative exposure,[23] while maintaining lawful content and upholding press freedom by allowing requests for the removal of links to personal information from search results.[24] Even if the original content remains accessible online, unless the overwhelming public interest demands its continued searchability, particularly in cases involving public figures.[25] Another illustrative example of this tension is the well-known Panama Papers case.[26] It included millions of documents revealing offshore businesses and individuals across the globe. Years later, a non-public individual called Ascanio asked for the removal of an internet article connecting his name to the news, asserting the right to be forgotten. The publisher refused to delete the article but de-indexed it from general search engines, making it accessible only through the newspaper's archives. This method protected Ascanio's reputation while still maintaining the historical record.[27] This aligns with the belief that the right to erasure should not be used to conceal important information from the public, seeing that the journalists are concerned that the *"right to be forgotten"* of the GDPR may hinder inquiries by making search engines delete important data, hence distorting narratives.[28] European courts balance privacy with free speech and public access. They protect personal data but allow important information.[29] On the other hand, the Japanese

[16] J.D., "Balancing a Right to Be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD", 178.
[17] Cambodia Constitution, Article 40.
[18] Cambodia Constitution, Article 41.
[19] Kamrul Faisa, "Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions," July, 2021, 2.
[20] Ministry of Post and Telecommunications, Cambodia Digital Government Policy 2022-2035, 2.
[21] Charter Of Fundamental Rights of The European Union, Article 11. European Convention on Human Rights, article 10.
[22] J.D., "Balancing a Right to Be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD", 179.
[23] Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014., Case C-131/12, 96.
[24] Google Inc. v Agencia, 98.
[25] Google Inc. v Agencia, 99.
[26] Will Kenton, "The Panama Papers Scandal: Who Was Exposed and Consequences", March 12, 2025.
[27] Giulio Ramaccioni, "Cases and Issues of the Right to Erasure (Right to Be Forgotten) Under the Article 17 Of Regulation (EU)", 43.
[28] Michael L. Rustad, and Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow", 374, vol.28.
[29] Giulio Ramaccioni, "Cases and Issues of the Right to Erasure (Right to Be Forgotten) Under the Article 17 Of Regulation (EU)", 43.

Supreme Court ruled against the right to erasure in a case involving an individual linked to child prostitution. The court determined that the public interest in maintaining the data outweighed the individual's request for its removal, as the information needed to be preserved for public interest even though he was arrested in 2011.[30]

The above cases exemplify the types of complexities Cambodia may face as it develops its legal framework on data privacy and the right to erasure as digital advancements occur daily. To address this, the government should establish a fair guide on the right to erasure so that it can coexist with other fundamental rights. Such a framework should precisely define the circumstances under which personal data can be erased. Including whether the information is in the public interest or involves an important individual. It should offer options other than complete erasure, such as de-indexing or limiting access to old but still important content. Additionally, there should be specific regulations in place to ensure journalistic freedom so that media outlets are not unfairly forced to take down content that adds to the public eye.

# IV. Challenges in Cross-Border Data Erasure

The problem of applying domestic laws beyond national borders in the digital world is a global challenge.[31] The courts all over are increasingly addressing significant concerns about the limits of global injunctions and whether there will be compatible rules for regulating the digital landscape in general.[32] With the limitation on cross-border transfer of data, Cambodia might face problems applying the right to erasure.[33] In 2022, nearly 70% of ministries in Cambodia relied on foreign cloud services due to the lack of a national data center, which often results in personal data being stored beyond Cambodia's jurisdiction and might undermine the effective enforcement of the right to erasure.[34] With that, once data is transferred abroad, the Cambodian regulator's jurisdiction and enforcement powers are limited. This creates a regulatory blind spot, making it difficult for Cambodian authorities to compel foreign entities to delete personal data upon request.

The right to erasure is better protected under the GDPR, particularly due to its strong data transfer mechanisms. Under the GDPR, data transfers from the EU to third countries can occur through several mechanisms. First, if a third country is granted an Adequacy Decision by the European Commission, it is recognized as providing a sufficient level of data protection, allowing transfers without additional safeguards, similar to data sharing within the EU.[35] In the absence of such a decision, transfers may still be permitted if appropriate safeguards are in place, such as standard contractual clauses approved by the EU,[36] binding corporate rules for affiliated companies, or following a code of conduct or certification mechanism with legally binding commitments from the recipient.[37] These mechanisms ensure that even when personal data leaves the EU, the rights of individuals, including the ability to request and enforce erasure of their data, are preserved and legally enforceable.

[30] Shizuo Fujiwara, "Current situation of discussions on Right to be forgotten in Japan", 2017.
[31] Faisal K., "Balancing between Right to Be Forgotten and Right to Freedom of Expression in Spent Criminal Convictions.", P62.
[32] Ibid.
[33] DLA Piper, "Data Protection Laws of the World", 20 January 2025, 11. https://www.dlapiperdataprotection.com/?t=transfer&c=KH
[34] Ministry of Post and Telecommunications, Cambodia Digital Government Policy 2022-2035, p12
[35] GDPR, Article 45.
[36] GDPR, Article 46.
[37] GDPR, Article 47.

To support the compliance with the right to erasure in the case of cross-border data, a strong mechanism for cross-data transfer is needed. Thailand's Personal Data Protection Committee (**PDPC**) published two subordinate regulations pertaining to cross-border transfers of personal data under the Personal Data Protection Act B.E. 2562 (2019) on December 25, 2023, by PDPC. These two regulations circle Articles 28 and 29 of the PDPA,[38] on conditions for cross-border transfer of personal data related to adequate data protection standards.[39] and how a controller or processor provides appropriate safeguards and ensures data subjects' rights and legal remedies.[40] Firstly, the PDPC establishes and revises a list of approved ("whitelisted") destinations and oversees compliance assessments and case resolutions related to cross-border data transfers.[41] And secondly, the Binding Corporate Rules (**BCRs**) and Appropriate Safeguards Notification issued by Thailand's Personal Data Protection Committee outline the criteria for safeguarding personal data transmitted among related enterprises or corporate groups.[42] On the other hand, under the Privacy Act 1988, there is a privacy on cross-border disclosure of personal information,[43] which requires the Australian government to comply.[44] However, there are data localization rules in Australia, such as the My Health Records Act 2012,[45] which mandates that certain operators and service providers cannot preserve, process, or regulate health records, which is sensitive information,[46] outside of Australia.

On that account, without cross-border legal cooperation mechanisms or strong domestic enforcement capabilities, Cambodia's right to erasure could be affected when data is held or processed internationally. Considering Cambodia's current data storage situation, Cambodia can look at the Australian My Health Records Act 2012 in storing sensitive data nationally by dividing what kind of sensitive data to be kept. Additionally, having something similar to a whitelist on where or what server the government can store the data internationally would reduce the burden of risking the control over the data, as they're most likely to abide by the GDPR.

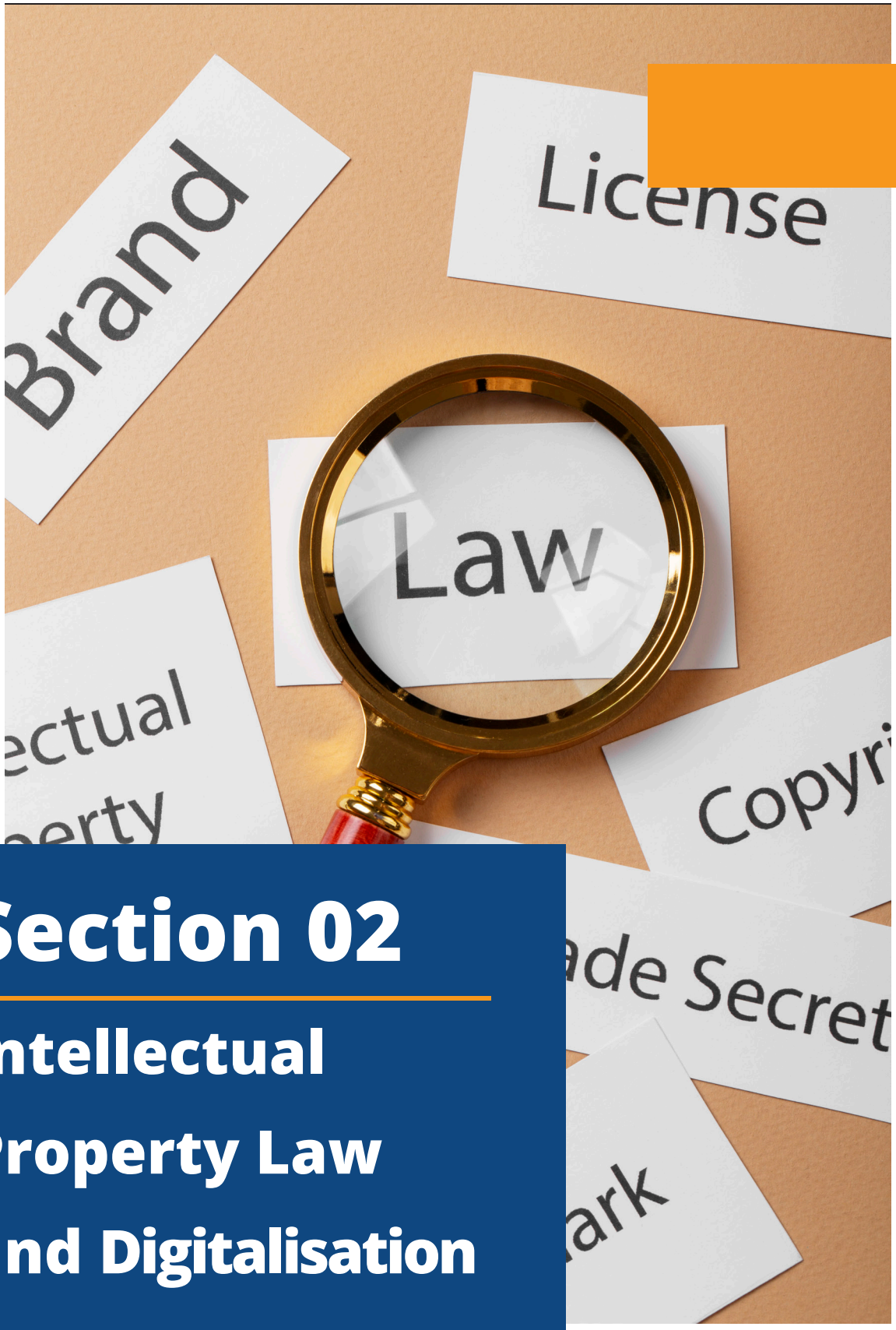
# V. Conclusion

As Cambodia becomes a more digitally connected society, the right to erasure becomes an important part of protecting people's privacy. The EU's GDPR is a positive example; however, there might be some parts that need clarification, especially for developing countries to follow. For instance, the complexity to find the correct balance between privacy and freedom of speech, define the duties of third-party controllers, and make sure that data is enforced across borders. As the government works on its personal data protection law, it should be clear on the legal gray areas, have enforceable rules, and observe the most effective international practices. This will protect people's rights, make the law more transparent, and assist individuals to trust Cambodia's digital future.

To ensure the ongoing advancement of this right, future studies need to explore several essential components. A comparative review of ASEAN data protection regulations could provide economical frameworks for Cambodia. Moreover, technical studies of data erasure in cloud systems and backups would aid in assessing enforcement longevity. Sector-specific impacts of the right to erasure—

[38] Muhamad Aziz and Ayman Falak Medina, "New Thai Law Targets Cross-Border Data Flows," ASEAN Briefing. May 7, 2024. https://www.aseanbriefing.com/news/new-thai-law-targets-cross-border-data-flows/.
[39] Thailand's Personal Data Protection Committee (PDPC), art 28.
[40] PDPC, art 29.
[41] Ibid.
[42] Ibid.
[43] Privacy Act 1988, Australian Government, Sub-Cl 8.1.
[44] Privacy Act 1988, SS 14–15.
[45] My Health Records Act 2012, Australian Government, S77.
[46] Privacy Act 1988, S6.

especially in journalism, healthcare, and education—should be examined to refine legal exemptions. Moreover, it is also important to pay attention to people's understanding of their rights to personal data and the duties and responsibilities of digital platforms that operate in Cambodia. Lastly, it will be important to examine how courts might implement this right, as it will be a new legal remedy in Cambodia. The conclusions will shape future interpretations of the law.




# Section 02

## Intellectual Property Law and Digitalisation

# The Absence of Legal Recognition and Enforcement Mechanisms for Publicity Rights in Cambodia's Digital Sphere


## RATANAK Prathnapitou

[Senior law student at the University of Arizona and AUPP]

Pitou is an alumnus of the AUPP Moot Court competition, having captained the AUPP team in the Phillip C. Jessup International Competition in his freshman year, and subsequently a competitor in the International Humanitarian Law Moot Court competition in his sophomore year. Currently, Pitou is pursuing his internship program at Rajah & Tann Sok & Heng Law Office, one of Cambodia's prestigious law offices, where he gets to work alongside experienced associates and attorneys in the areas of capital markets and real estate.


# I. Introduction

The digital age has made personal identity a valuable commodity for everyone. Currently speaking, individuals' names, images, voices, and persona indicia are now routinely used for commercial purposes, mostly by businesses, on digital advertising platforms, and even by algorithms, often without their prior consent. In response, many jurisdictions have recognized the "Right of Publicity", defined variously as the inherent right of every human being to control the commercial use of their identity,[1] the commercialization of popularity, or the media exploitation of privacy.[2] Despite different interpretations, these rights derive from the 'right to privacy' and the 'right to let alone' which apply to everyone, regardless of their identity's value, and fame.[3]

However, in Cambodia, these rights remain without any explicit legal recognition,[4] leaving individuals increasingly vulnerable to exploitation, especially in the rapidly evolving digital ecosystem. With the current existence and growing popularity of artificial intelligence (**AI**), technology has intersected with personal identity, raising complex ethical legal questions.[5] Emerging deceptive practices such as "deepfakes"[6] and "digital clones" have enabled the widespread appropriation of identities for commercial benefits, further

[1] Marlan, Dustin. "The Dystopian Right of Publicity." Journal of Berkeley Technology Law 37, no. 2 (2022): 805.
[2] Black, Gillian, Publicity Rights and Image: Exploitation and Legal Control (Oxford: Hart Publishing, 2011), p.11.
[3] Luthra, Samarth Krishan, and Vasundhara Bakhru. "Publicity Rights and the Right to Privacy in India." Journal of National Law School of India Review 31, no. 1 (2019): p.126.
[4] BNG Legal, "IP Protection in Cambodia (Mar, 2024)," BNG Legal, March 2024, https://bnglegal.com/index.php/ip-protection-in-cambodia-mar-2024/.
[5] Eliana, Torres. "From Deepfakes to Deepfame: The Complexities of the Right of Publicity in an AI World." Journal of Landslide 16, no. 2 (December 2023): p.1.
[6] According to the US Copyrights Office, "digital replicas" or "deepfakes" are videos, images, or audio recordings that have been digitally created to accurately but falsely depict an individual by feeding large amounts of photo or voice samples into a "neural network" and 'training it' to index and reconstruct patterns, that typically generate faces. U.S. Copyright Office. Copyright and Artificial Intelligence, Part 1: Digital Replicas. Washington, D.C., July 2024 https://www.copyright.gov/AI.

complicating the enforcement of personal rights in the digital space. In this context, Cambodia's current legal framework must be scrutinized for its capacity to safeguard Publicity Rights.

This brief aims to (**II**) identify the gaps in Cambodia's current legal framework; (**III**) examine a comparative legal analysis of how other jurisdictions, namely the US, the UK, France, and Germany protect Publicity Rights in the digital realm, and propose an adequate recognition of this right to be a legally enforceable concept in digital spaces, into Cambodia's current draft laws, particularly the Draft Personal Data Protection Law **(PDPL)** and the Draft Cybercrime Law **(CL)**.

# II. Gaps and Loopholes in Cambodia's Current Legal Landscape

## 1. The Consitution and Civil Code Blindspot

Cambodia's Constitution provides a foundational "right to privacy" that protects the 'privacy of correspondence and communications' and a 'respect for private life'.[7] In a complementary manner, Article 10 of the Cambodian Civil Code recognizes individual "personal rights", including the right to freedom, identity, dignity, privacy, and other personal benefits or interests. Importantly, attached to these rights, the Civil Code also grants rights-holders the ability to (1) seek injunctions against infringing acts,[8] (2) request the elimination of the act,[9] and (3) claim damages for violation of personal rights.[10] The exercise of the right to damages must be in accordance with the provisions of tortious acts under the code.[11]

However, the issue lies in the ambiguity of the legal grounds for a claim. Suppose that a plaintiff wishes to bring an action citing a 'violation of publicity rights', due to an unconsented use of his image for an online advertisement endorsing a particular product or service, on what legal basis does he sue? This legal blind spot undermines the legal protection for these rights. Furthermore, the lack of a codified cause of action in Cambodia's civil law system frustrates judicial interpretation that effectively forces judges to stretch general privacy clauses into contexts they were never intended to regulate, such as A.I generated images and videos, cloning, deepfakes, or unauthorized algorithmic monetization of personal likenesses. While Cambodia's civil law structure aligns with personality rights traditions like Switzerland's, it still lacks the doctrinal clarity or interpretive guidance necessary to respond effectively to identity exploitation in the digital age.[12] As a result, the plaintiff would have to resort to other related laws and regulations that revolve around the protection of Publicity Rights.[13]

## 2. Protection Under the Criminal Code

The Cambodian Criminal Code offers limited protection for personal identity, primarily through provisions on defamation,[14] public insult,[15] and private recordings.[16] However, these provisions are

[7] The Constitution, Article 40
[8] Civil Code, Article 11.
[9] Civil Code, Article 12.
[10] Civil Code, Article 13.
[11] Explanatory Notes on Cambodia Civil Code, Article 13, pp.7-9.
[12] Phin, Sovath, "Privacy and Data Protection in the Digital Age: A Holistic Approach to Privacy and Data Protection in Cambodia," in Law in the Digital Age: Protection of Consumer Rights, ed. (2021), p.63.
[13] Black, G. "Publicity and Image Rights in Scots Law." Journal of Edinburgh Law Review 14, no. 3 (2010): p.375.
[14] Criminal Code, Article 305.
[15] Criminal Code, Article 307.
[16] Criminal Code, Article 301.

designed to safeguard reputation, not to address the economic harm caused by the unauthorized use of identity. For example, if a person's voice or image is digitally used in an advertisement without their consent, but without defamatory content, such use would fall outside the scope of criminal liability. Therefore, the code does not recognize the autonomous economic value of personal identity,[17] nor does it criminalize its misappropriation for profit under false endorsement or synthetic influence.

## 3. E-commerce and Consumer Protection Laws and Regulations: A Misdirection

Article 22 of the E-Commerce Law prohibits using another person's identity, electronic signature, or address in bad faith or without permission, whether for commercial or non-commercial purposes.[18] At first glance, this provision seems promising. However, if construed narrowly, this provision intends to restrict the use of 'stolen identity' to fraudulent transactional conduct. Articles 24 and 25 of the Law further provide liability and take-down obligations for service providers that have actual knowledge of "unlawful content".[19] However, since publicity rights violations are not codified as unlawful, such content does not fall under the obligation that triggers liability.

The Consumer Protection Law is similarly limited in scope. The Law prohibits unfair acts regarding goods and services and misleading representations.[20] Subsequent Sub-Decree,[21] and Prakas,[22] have explicitly prohibited 'forced' and 'involuntary' advertisement of individuals by commercial businesses. Violation of these provisions is subject to an interim fine not exceeding KHR 50,0000,000,[23] and suspension or revocation of their advertisement licenses.[24] However, these provisions are limited to avoid consumer confusion and address their rights, not to the person whose image or likeness is being exploited commercially.[25] The focus of the Right of Publicity is not on the consumer's interest, but rather on the exploited person's interest in controlling and benefiting from the economic value of his identity.[26]

## 4. Intellectual Property Law: Copyrights and Trademark Structral Barrier

The purpose of the Law on Copyright and Related Rights (**Law on Copyrights**) is to promote creativity and recognize authorship,[27] which is ill-equipped and beyond the scope to preserve Publicity Rights.[28] The Law defines "authors",[29] and "performers",[30] as someone who creates or performs protectable works. However, a person whose face is used in a digital ad, or whose voice is cloned through A.I, is neither an author nor a performer unless they contributed to a protectable work or gave a real performance. Consequently, attached rights like 'moral' and 'economic' rights, such as remuneration,[31] that are intended to protect the integrity of the work and prevent distortion, are inapplicable.[32] Even when photographs are involved,[33] the Law generally grants ownership to the photographer instead of the subject, leaving individuals with no control over the commercial use of their image.[34]

[17] Bariach, Ben, Bernie Hogan, and Keegan McBride. "Towards a harms taxonomy of ai likeness generation". (2024). https://doi.org/10.48550/arXiv.2407.12030.
[18] Law on E-Commerce, Article 22.
[19] Law on E-Commerce, Article 24 (1).
[20] Law on Consumer Protection, Article 10; Article 11; Article 12.
[21] Sub Decree No. 232 on the Management of Commercial Advertising on Products and Services dated 04 November 2022, Article 17(6)
[22] Prakas No. 095 on Unfair Practices in Business Related to Advertisements and Sales Promotions dated 12 April 2024, Article 6.
[23] Law on Consumer Protection, Article 44.
[24] Sub Decree No. 232, Article 19.
[25] Law on Consumer Protection, Article 9.
[26] Fernandez, Cristina. "The Right of Publicity on the Internet." Journal of Marquette Sports Law 8, no. 2 (Spring 1998): p.319.
[27] Law on Copyrights and Related Rights, Article 1.
[28] Dogan, Stacey L., and Mark A. Lemley. "What the Right of Publicity Can Learn from Trademark Law." Journal of Stanford Law Review 58, no. 4 (February 2006): pp.1180-1190.
[29] Law on Copyrights, Article 2(b).
[30] Law on Copyrights, Article 2(e).
[31] Law on Copyrights, Article 49.
[32] Law on Copyrights, Article 18.
[33] Law on Copyrights, Article 7.
[34] Farish, Kelsey. "Do Deepfakes Pose a Golden Opportunity? Considering Whether English Law Should Adopt California's Publicity Right in the Age of the Deepfake." Journal of Intellectual Property Law & Practice 15, no. 1 (2020): p.43.

Law Concerning Marks, Tradenames, and Acts of Unfair Competition (**Law on Trademark**), on the other hand, offers better protection than Copyright Laws,[35] though it is designed primarily to protect commercial marks or tradenames and prevent unfair competition.[36] Likewise, registration of a "mark" may prevent others from using identical or confusingly similar marks.[37] However, suppose that a person's names, voices, and likeness fall under the definition of "mark" under the Law,[38] it is not ideal for people to register their personalities, nor is there a personality asset registry system. Article 23 additionally prohibits acts of unfair competition, such as acts that create confusion, false allegations, and misleading facts about the goods or services to the public. Like the Consumer Protection Law, this provision is designed to protect the commercial marketplace from deceptive practices. Thus, instead of the dignitary or economic interest of the person being impersonated, the provision concerns deception and market integrity, providing an indirect protection.

# III. Comparative Models in Publicity Rights Protection

## 1. The Us: Golden Rule for Publicity Rights Recognition

The US offers one of the most developed frameworks for protecting Publicity Rights,[39] even though it lacks a unified federal statute.[40] Most states recognize these rights through either statute or common law cases (*prima facie*), with varying degrees of protection.[41] This section will analyze how the US, through state laws and common law cases, protects Publicity Rights and its approach toward the emergence of A.I and deepfakes.

### A. Publicity Rights Protection Across Different Us State Laws

California Civil Code §3341 provides that any person who (1) knowingly uses another's name, voice, signature, photograph, or likeness, in any manner (2) for purposes of advertising or selling goods or services, (3) without such person's prior consent (4) shall be liable for any damages sustained by the person or persons injured as a result thereof.[42] This section establishes civil liability for the unauthorized commercial usage of another's image without consent and recognizes the resulting conversion of potential economic value in said image.[43] Exceptions apply to news, public affairs, or sports broadcasts or accounts, or with a political campaign.[44] This protection also extends 'posthumously' through §3344.1, which grants heirs and legal representatives the authority to control and seek damages for unauthorized commercial uses of a deceased individual's persona, including 'digital replica'.[45] Similar effort was seen in the New York Civil Code,[46] where scripted audiovisual works or musical performances involving fictional portrayals of individuals through digital replicas powered by AI and deepfakes technologies are strictly prohibited.[47]

Tennessee, on the other hand, just enacted a comprehensive 'Ensuring Likeness Voice and Image Security Act' (**ELVIS Act**) to combat the growing threat of unauthorized identity replication in the

[35] Dogan, Stacey L., and Mark A. Lemley. "What the Right of Publicity Can Learn from Trademark Law.", op.cit., p.1190.
[36] Law on Trademark, Article 1.
[37] Law on Trademark, Article 11.
[38] Law on Trademark, Article 2.
[39] Adrian, Angela. "Trademark Dilution, Right of Publicity, Image Rights: A Comparative Analysis of US, UK, Australian and Japanese Law". Icondia, March 2014., p.3.
[40] Muchiri, Moses. "In Search for a Jurisprudential Justification for the Recognition of a Right of Publicity in Kenya." Journal of GRUR International 69, no. 6 (2020): p.599.
[41] Ibid.
[42] California Civil Code §3341.
[43] Farish, Kelsey. "Do Deepfakes Pose a Golden Opportunity? Considering Whether English Law Should Adopt California's Publicity Right in the Age of the Deepfake.", op.cit., p.42.
[44] CACI No. 1804A. Use of Name or Likeness (Civ. Code, § 3344), https://www.justia.com/trials-litigation/docs/caci/1800/1804a/.
[45] California Civil Code §3344.1(a)(2)(A)(i).
[46] New York Civil Code §50-f.
[47] Chawki, Mohamed. "Navigating Legal Challenges of Deepfakes in the American Context: A Call to Action." Journal of Cogent Engineering 11, no. 1 (2024): p.8.

digital age.[48] The ELVIS Act's most notable cause of action is that it allows for civil action against anyone who distributes or provides access to 'software, algorithms, or tools' specifically designed to produce "unauthorized replicas" of a person's voice, image, or likeness.[49] Legal accountability is expanded not only to those misusing digital identities but also to those enabling such misuse (service providers) through technological means. Additionally, the person who commits unauthorized use may be deemed to have committed a Class A misdemeanor and held criminally responsible.[50]

### B. The Common Law Approach in Establishing a *Prima Facie* Case

While several U.S. states have codified the Right of Publicity, many continue to recognize and enforce it as a matter of common law, rooted in tort principles (privacy and dignitary harms)[51] rather than statutory text.

To prevail on a prima facie case for liability of infringement of the Rights to Publicity, a plaintiff must plead and prove the following basic elements:[52]

**(1)** Validity: Plaintiff owns an enforceable right in the identity or persona of a human being; and

**(2)** Infringement:

**(A)** Defendant, without permission, had used some aspect of identity or persona in such a way that the plaintiff is identifiable from the defendant's use; and

**(B)** Defendant's use is likely to cause damage to the commercial value of that person.

A landmark case illustrating the enforcement of common law Publicity Rights is *Zacchini v. Scripps-Howard* (1977), and *White v. Samsung* (1992), where the Court held that unauthorized broadcast of a performer's act and recognizable representation,[53] violated the plaintiff's Publicity Rights.

## 2. The European Approach to Publicity Rigts Recongnition and Its Relevancy to Cambodia's Current legislation

### A. Frence's Dignity-Based and Germany's Constitutional Expression of Personality

Unlike the U.S., French law employs a dualistic model to protect Publicity Rights: the right to one's image and the right over one's image.[54] The system is dignity-focused rather than market-driven since it treats image misuse as a personal and moral intrusion rather than a loss of commercial opportunity.[55] Furthermore, Article 9 (Rights to Privacy) of the Civil Code and Article L.226-1 (Offence against Privacy) of the Criminal Code prohibit the dissemination of a person's private information without their consent. Additionally, the Commission Nationale de l'Informatique et des Libertés was established to oversee human identity, rights, and privacy, or public liberties, in the development of information technology.[56] The CNIL is also a national authority in charge of monitoring France's compliance with the GDPR regarding the processing and collection of personal data. [57]

Furthermore, Germany offers one of the strongest protections for personality rights within the EU,

[48] Harbin, Ashley. "ELVIS Act: Tennessee Safeguards Against Deepfakes."Adams and Reese LLP, March 26, 2024. https://www.adamsandreese.com/insights/elvis-act-tennessee-safeguards-against-deepfakes.
[49] Tennessee Code §47-25-1105 (a)(3).
[50] Tennessee Code §47-25-1105 (b).
[51] Marlan, Dustin. "The Dystopian Right of Publicity.", op.cit., pp.12-14.
[52] McCarthy, J. Thomas, The Rights of Publicity and Privacy, 2nd ed., vol. 1 (St. Paul, MN: Thomson Reuters, 2017), § 3:2, p.115.
[53] Dogan, Stacey L., and Mark A. Lemley. "What the Right of Publicity Can Learn from Trademark Law.", op.cit., p.1195.
[54] Black, G. "Publicity and Image Rights in Scots Law.", op.cit., p.373.
[55] Cantero, Inés, Stephan Dittrich, Sara Garcia Alvarez, Regina Herzig, and Lukas Illich. "Exploiting Publicity Rights in the EU." EIPIN Report (April 2010): p.7.
[56] Ibid.
[57] DLA Piper. "France." Data Protection Laws of the World, p.10. https://www.dlapiperdataprotection.com/?t=authority&c=FR#insight.

largely due to its constitutional framework. German courts have developed the doctrine of "Allgemeines Persönlichkeitsrecht" (general personality right) under Articles 1(1) and 2(1) of the Basic Law (**Grundgesetz**), which uphold human dignity and the right to self-determination.[58] These rights are enforced through civil law instruments such as Sections 823(1) and 1004 of the Civil Code and Section 22 of the Copyright Act (**KUG** Landmark cases, such as Franz Beckenbauer and Nena, have drawn clear lines against unlicensed merchandising and advertising that exploit fame for profit without consent.[59]

Both civil law jurisdictions offer valuable reference points for Cambodia to seek a robust framework in protecting Publicity Rights. These jurisdictions show how broad civil and criminal provisions, backed by constitutional protection, can be interpreted by the court to protect personality rights even without a dedicated publicity statute. Given that Cambodia is on the verge of drafting a complete Law on Cybercrime, acts of identity misuse through technological tools like A. I shall be criminalized and properly defined to avoid ongoing violations.

Although Cambodia does not yet have a body like CNIL, a National Data Regulator of Personal Data is expected following the adoption of the Draft PDPL. While the GDPR does not directly protect the Right of Publicity, several of its provisions indirectly protect personal identity from unauthorized commercial use. For instance, Article 4(1) broadly defines personal data to include information relating to an identified or identifiable person, encompassing images, names, voices, and likenesses. Lawful processing of such data often necessitates explicit consent.[60] Additionally, individuals have rights attached to their data, such as the (1) right to be forgotten,[61] (2) the right to object,[62] (3) the right to damages.[63] Therefore, with the influence of the GDPR, Cambodia's Draft PDPL can be a means to protect Publicity Rights.

### B. United Kingdom: A Flexible IP-Based Framework

The UK does not recognize a distinct Right of Publicity. Instead, it relies on a patchwork of doctrines such as the tort of passing off, breach of confidence, and privacy rights under the Human Rights Act 1998.[64] Courts continue to resist creating a freestanding publicity tort, relying instead on adaptations of IP and privacy law. The UK's reliance on different doctrines offers Cambodia a pragmatic model for adapting to its existing IP Laws.

Likewise, Cambodia could follow the UK's flexible approach by interpreting unfair competition, false endorsement under its trademark law, and including breach of confidence into its tort system. This can cover misappropriation of likeness in digital advertising or influencer marketing and provides Cambodia with interim strategies to leverage existing IP and Consumer Protection laws while drafting considerate laws such as the PDPL and the CL.

# IV. Conclusion

To conclude, this brief has demonstrated that Cambodia's current legal framework remains inadequate in addressing the unauthorized commercial use of personal identity in the digital realm. As

[58] Coors, Corinna. "Celebrity Image Rights versus Public Interest: Striking the Right Balance under German Law." Journal of Intellectual Property Law & Practice 9, no. 10 (2014): pp.835-836.
[59] Ibid., pp.837-838.
[60] GDPR, Article 6(1).
[61] GDPR, Article 17.
[62] GDPR, Article 21.
[63] GDPR, Article 82.
[64] Cantero, Inés, Stephan Dittrich, Sara Garcia Alvarez, Regina Herzig, and Lukas Illich. "Exploiting Publicity Rights in the EU.", op.cit., p.5.

digital technologies like A.I. and deepfakes accelerate, the legal silence surrounding Publicity Rights leaves individuals vulnerable to economic and dignitary harm.[65] Moving forward, Cambodia faces two strategic alternatives.

The first is to adopt statutory recognition of Publicity Rights, as seen in U.S. States laws, where legislation clearly defines and enforces the right to control one's identities for commercial use. The second approach is to reinterpret existing Cambodian laws by drawing from comparative jurisdictions such as the U.S. *prima facie*, and the European approach to offer limited but functional remedies.

For Cambodia, the choice is not merely between codification and reinterpretation—it is a test of whether the legal system is prepared to confront emerging harms with coherence and urgency. Continued inaction will not only entrench legal ambiguity but also risk normalizing the exploitation of identity as an unregulated commercial practice.

[65] Beverley-Smith, Huw. The Commercial Appropriation of Personality, Cambridge Intellectual Property and Information Law, vol. 1 (Cambridge: Cambridge University Press, 2002), p.8.

# The Copyright Dilemma: a Critical Approach to Ownership of AI-Generated Content


## CHES Sindy

[Undergraduate in French and Khmer law of RULE]

She represented Cambodia at the 2024 International Conference on E-Commerce in China, and subsequently participated in the 2025 International Criminal Law Moot Court in the Netherlands. In addition, she completed internships at two leading law firms, HBS LAW and Sethalay Law Office, where she gained valuable hands-on experience in legal practice. Most recently, she was awarded a scholarship to pursue a Master's degree in Business Law at Jean Moulin Lyon 3 University in France.


# I. Introduction

In the digital age, technological progress, particularly in artificial intelligence (**AI**), is advancing beyond expectations. AI, defined as a machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments,[1] is now generating numerous literary, artistic, and musical works. This development expands creative tools for individuals and institutions while simultaneously raising critical legal questions regarding copyright protection.

While Cambodian legislation has not yet established a specific legal position on the use of AI, foreign jurisdictions, such as the United States,[2] and the European Union,[3] have adopted a limited framework in which AI-generated content may receive copyright protection, but only if it meets a minimum threshold of human creativity.

Meanwhile, Article 7 of the 2003 Cambodian Law on Copyright and Related Rights protects computer programs, but not content generated by such programs. This omission is understandable, as AI-generated content was unforeseen at the time. However, it leaves a legal ambiguity regarding the applicability of this law to AI-generated content, an issue that remains

[1] Association of Southeast Asian Nations (ASEAN), "ASEAN Guide on AI Governance and Ethics", 2024, p. 9.
[2] United States Copyright Office, "Copyright and Artificial Intelligence", Report of the register of copyrights, part 2: Copyrightability, 2025.
[3] Infopaq International A/S v Danske Dagblades Forening, Case C-5/08, CJEU, 2019.

unresolved in the absence of judicial interpretation.

By analyzing this legal challenge within the framework of copyright law, this brief aims to assess the applicability of copyright protection to content generated by AI, drawing on multiple cases from U.S. courts to clarify the legal issues. As home to leading AI companies such as OpenAI, Google, IBM, and Nvidia, the United States has experienced a significant rise in litigation involving AI-generated works and alleged copyright infringement.[4] In response, the country has developed a robust legal framework, notably through initiatives by the U.S. Copyright Office, including its two-part reports on digital replicas and the copyrightability of AI-generated content. With 82 AI-related policies and strategies adopted in 2024, the United States ranks first globally in terms of legal instruments addressing AI.[5] Its evolving jurisprudence provides a valuable foundation for comparative analysis and can serve as a model for Cambodia as it prepares for an AI-integrated future.

This brief also seeks to identify the current vulnerabilities of Cambodian copyright law in the face of technological change, particularly concerning the use of AI as a creative tool for modern authors.

Since copyright is reserved to the author of an original work, it is essential to clarify the legal uncertainties surrounding authorship in the context of AI-generated content (**II**), and to assess whether such content meets the criteria of originality (**III**). While these two concepts generally suffice to determine protection, this brief finds it desirable to examine unresolved issues of copyright infringement (**IV**), before concluding with recommendations for a fair balance between human creativity and the rights of authors (**V**).

# II. Legal Challenges in Determining the Rightful Authorship of AI-generated Content

By addressing the challenge of authorship in AI-generated content, this legal brief aims to analyze, from a legal perspective, who the true author of the generated content is. Identifying the author is essential for determining who is entitled to the corresponding legal protections, whether it be the AI itself, the user, or the developer. This determination is also crucial for establishing who has the legal standing to file a lawsuit in the event of copyright infringement.

Pursuant to Article 11 of the 2003 Cambodian Law on Copyright and Related Rights, the title of author belongs to the natural person or persons in whose name the work is created and disclosed. The phrase *"natural person or persons in whose name the work is created and disclosed"* is further clarified in Article 13 of the same law as referring to a *"natural person or legal person."* From these provisions, the concept of authorship is granted only to natural persons or legal entities. This raises the question of whether AI can be recognized as a natural or legal person.

By its nature, AI is a computer system created and trained by humans. No legal provision has ever granted legal personality to a computer system, primarily because, in line with Article 46 of the 2007

[4] Kate Knibbs, "Every AI Copyright Lawsuit in the US, Visualized", Wired, December 19, 2024, https://www.wired.com/story/ai-copyright-case-tracker/.
[5] "AI Laws Around the World", AIPRM, https://www.aiprm.com/ai-laws-around-the-world/ .

Cambodian Civil Code, it lacks rights and obligations independent of its developer and user. This absence of independence could never allow AI to be regarded as a legal person. A similar issue regarding legal personality was addressed in the well-known "Monkey Selfies" case, *Naruto v. David Slater.*[6] (No. 16-15469) before the United States District Court. The court examined whether a monkey could hold the copyright to photographs it had accidentally taken when David Slater left his camera unattended. The court ruled, *"the monkey lacked statutory standing because the Copyright Act does not expressly authorize animals to file copyright infringement suits.*[7]*"*

This case demonstrates that an entity cannot acquire legal personality without legal recognition. Since a monkey, despite possessing emotional qualities comparable to those of humans, was denied legal personality, it is even less conceivable for a computer program, which operates solely under a user's command, to be granted such status. It is legally implausible for AI to assume the obligations and responsibilities required for legal personality. Therefore, AI cannot be considered the author of any copyrighted work. Moreover, changing laws to allow AI ownership would involve significant costs without obvious benefits.[8]

So, what about AI developers? Can they be considered the authors of AI-generated content? To answer this question, it is crucial to determine whether AI functions independently from its developers. AI is *"a branch of computer science concerned with creating machines that can think and make decisions independently of human intervention.*[9]*"* It operates through a system called an "*algorithm,*" which is defined as *"the programming that tells the computer how to learn to operate on its own.*[10]*"* Analyzed from these definitions, the AI developer cannot be the author of the generated content, owing to the fact that AI functions independently from its developers and relies solely on the pre-created algorithm to accomplish assigned tasks on its own. Attempts by developers to claim copyright over AI-generated content have been denied by the United States Copyright Office and the United States District Court in the case of *Thaler v. Perlmutter.*[11]

After analyzing the possibility of granting authorship to the AI or its developer, the only remaining candidate for authorship is the AI user, as they are the ones who benefit directly from the AI service. However, even though users may be involved and exert some control over the AI-generated content, there are limitations; not all users are entitled to ownership of the resulting content. It is important to distinguish between those who use AI merely as a tool to refine their ideas and those who rely entirely on AI to generate a fully finished product.

Meanwhile, no legal provision prohibits an author from seeking assistance during their creative process. On the contrary, what matters for copyright protection is the originality of the underlying idea. To address this matter, a detailed analysis of the originality of AI-generated content is essential and will be provided in Section II.

[6] Naruto v. David Slater, 16-15469 (9th Cir. 2018).
[7] Ibid.
[8] Ryan Abbott, "The Artificial Inventor Project", WIPO Magazine, December 11, 2019, https://www.wipo.int/en/web/wipo-magazine/articles/the-artificial-inventor-project-41111.
[9] Tableau from Salesforce, "Artificial intelligence (AI) algorithms: a complete overview", https://www.tableau.com/data-insights/ai/algorithms.
[10] Ibid.
[11] Thaler v. Perlmutter, 22-1564 (D.D.C. 2023).

# III. Ambiguity of Originality in AI-generated Content and Its Impact on Copyrightability

Copyright is granted to the "author" of an "original" work. To claim copyright over a created work, the author must provide proof of the content's originality. Nevertheless, how can originality be determined when a work is created entirely by AI or with the assistance of AI?

Pursuant to Article 4 of the 2003 Law on Copyright and Related Rights of Cambodia, a work shall be deemed original if it represents the genuine intellectual creation of its author. Additionally, Article 5 of the same law states that *"A work is deemed created, independently of all public disclosure, by the sole fact of the realization, even if incomplete, of the author's idea."* These provisions emphasize the importance of the human intellect behind a work. The human intellect is defined as the application of intellectual effort, creativity, or the exercise of mental labor, skill, or judgment.[12] This is the core element of originality, which suggests that AI-generated content may be eligible for copyright protection as long as the underlying idea is an original intellectual effort attributable to a specific author.

The fact that a work is not physically created by the author does not affect the attribution of copyright protection. A remarkable example is *Sol LeWitt*, an American conceptual artist, who was granted copyright protection for his written instructions, even though he did not personally draw or paint the resulting artworks. Works produced based on his instructions are considered authentic and are accompanied by certificates of authenticity.

In the case *Thaler v. Perlmutter,*[13] the court addressed the question of the eligibility of AI-generated works for copyright protection. The decision highlighted the importance of human involvement, as copyright protection is granted to a human author, not the machine, even though the content is machine-generated. However, to what extent must a human author be involved in their work to qualify for copyright protection? To explore this issue, two examples of AI-generated output, each reflecting different degrees of human input, will be examined.

Example 1:

*"Draw me a red rose with two bees surrounding it, one on the left petal and the other flying, protected under a clear glass in a room full of other flowers".*

*Figure : ChatGPT (AI) generated image*

[12] Global Yellow Pages Limited v. Promedia Directories PTE LTD, SGCA 28 (2017), par. 24.
[13] Thaler v. Perlmutter, 22-1564 (D.D.C. 2023).

Example 2:

*"Draw me a flower".*

*Figure : ChatGPT (AI) generated image*

The first prompt demonstrates the author's idea of the image. It indicates that, while writing the prompt, the author already has a clear concept of what the picture should look like by providing a detailed description. Only certain aspects, such as the color and the number of flowers in the background, are left to the AI's interpretation. In this case, the author's original idea is embedded in the prompt itself, and AI functions merely as an assistive tool to realize that vision. On the contrary, the second prompt does not illustrate the author's concrete idea of the picture, and AI is in control of the whole creation process.

This implies that the term "original work" cannot apply equally to someone who simply provides a generic command and to someone who offers a detailed, specific prompt. The law should establish clear limitations on the required level of human involvement in the creation process to determine both originality and authorship because the copyright should not be granted to someone with a bare minimum of creative idea, as in the example above, a generic prompt like "draw me a flower" is something anyone, even a six-year-old child, could come up with. This lack of creativity and originality results in an authorless work, regardless of how aesthetically pleasing, useful, or valuable it may be.[14] This means, *"if no one owns these inventions, they will fall into the public domain."* [15]

Problems arise when AI-generated content is indistinguishable from human work. For example, *Zarya of the Dawn,*[16] by Kristina Kashtanova was initially registered for copyright, but after it was revealed that AI tool Midjourney created the images, the U.S. Copyright Office revoked the original certificate and reissued one covering only text, selection, coordination, and arrangement of the written and visual elements.[17] This case highlights the challenges of applying copyright law to AI-generated content. As a result, judges must assess originality on a case-by-case basis, determining the extent of human involvement required for copyright protection, an issue that has yet to be addressed in Cambodian jurisprudence.

Since the originality of AI-generated content is uncertain, determining whether such content constitutes copyright infringement is even more complex. This issue will be addressed in Section.

[14] David Tan, "AI and Copyright: Death of the Author?", Law Gazette, November 2022, https://lawgazette.com.sg/feature/ai-and-copyright-the-death-of-author/.
[15] Trevor F Ward, "DABUS, An Artificial Intelligence Machine, Invented Something New and Useful, but the USPTO Is Not Buying It", Maine Law Review, 2023, p. 84.
[16] United States Copyright Office to Van Lindberg, Washington DC, February 21, 2023.
[17] Ibid., p.1.

# IV. Unauthorized Use of Authentic Content in the Creation of AI as a Matter of Copyright Infringement

As a computer program created by humans, AI is accused of being an unoriginal productivity machine. This criticism stems from the fact that AI must be trained on large datasets, raising uncertainty as to whether all the data used has been lawfully obtained and whether AI-generated content may reproduce existing copyrighted material, thereby potentially constituting copyright infringement (Sub section 3.1), subject to certain exceptions such as the doctrine of *Fair Use* (Sub section 3.2).

## 1. Copyright Infringement and Liability in AI-generated Content

As previously mentioned, because AI systems require vast amounts of data for training, some of the data may inevitably include copyrighted material. This situation raises important legal questions concerning copyright infringement and liability. How exactly can AI-generated content infringe upon copyrighted works? Who should be held accountable in the event of such infringement?

As Nizel Adams, CEO and principal engineer at AI consultancy Nizel Corps, stated: *"The problem with AI-generated content is that users don't know exactly where the AI is sourcing things from and which parts of the content it creates are original or merely pulled from another piece of copyrighted content, or even another person's AI-generated artwork on the platform".*[18] Since AI is created by humans to mimic human-like qualities, it must be trained using real data, which may include works from real artists, sometimes without their consent. For instance, OpenAI has used a collection of over 7,000 unique unpublished books to train GPT-1. These books were copied from a website called Smashwords.com and used without consent, credit, or compensation to the authors.

In addition, in the case of *Authors Guild v. OpenAI,*[20] a group of authors of copyrighted works of fiction sued OpenAI, alleging that their works were used to train its "large language models" without their consent. The court ruled that OpenAI was liable for copyright infringement as it had contributed to and directly assisted in the infringement of the author's works by providing the necessary resources and support for the training.

The case underscores two key principles. First, the rights of creators must remain protected, and the unauthorized use of their works can result in liability for the user. Second, since AI is merely a tool, its developer is responsible for any infringement caused by their products, even though they do not necessarily own the copyright to the content it generates.

In most cases, AI companies are sued for copyright infringement as they use copyrighted works of original authors to train their systems. This practice can result in the replication of distinctive styles, expressions, or information in AI-generated outputs, as illustrated in cases such as *Andersen v. Stability AI Ltd.*[21], *Tremblay v. OpenAI, Inc.*[22], and *Getty Images (US), Inc. v. Stability AI, Inc.*[23]

[18] George Lawton, "Is AI-generated content copyrighted?", Informa TechTarget, 2024, https://www.techtarget.com/searchcontentmanagement/answer/Is-AI-generated-content-copyrighted.
[19] Tremblay et al v Open AI, 3:23-cv-03223 (N.D. Cal., 2023), par. 28-29.
[20] Authors Guild v. OpenAI, 1:23-cv-8292 (S.D.N.Y, 2023).
[21] Andersen v. Stability AI Ltd., 23-cv-00201-WHO (N.D. Cal., 2024).
[22] Tremblay v. OpenAI, Inc., 3:23-cv-03223 (N.D. Cal., San Francisco Div., 2023).
[23] Getty Images (US), Inc. v. Stability AI, Inc., 1:23-cv-00135-UNA, (D. Del., 2023).

Although holding the AI system itself liable is currently impossible, due to its lack of legal personality, shifting the responsibility to users may be even more unfair. In most cases, users have no knowledge of the training data used to develop the AI and no access to the specific copyrighted works that may have been reproduced in the output.[24] Therefore, imposing liability on users who act in good faith and without intent to infringe could only lead to unjust outcomes.

## 2. The Possibility of Applying the Fair Use Doctrine to AI-generated Content

While the issue of copyright infringement in AI-generated content is being addressed, judges and legislators should also consider the potential application of the Fair Use doctrine to such content. In particular, can the use of copyrighted material for training AI systems be considered a legitimate form of fair use?

As a legal doctrine that promotes freedom of expression by permitting the unlicensed use of copyright-protected works in certain circumstances,[25] *Fair Use* is considered an exception to copyright protection. It provides creators with access to existing works, allowing them to draw inspiration from original content without infringing upon the rights of the copyright holder.

In the view of the United States Circuit Judge in *Thomson Reuters v. Ross Intelligence,*[26] the court considered four factors when assessing fair use: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion used in relation to the original work, (4) the effect of the use on the potential market of the copyrighted work.

The court ruled against *Ross Intelligence*, as its use was commercial and non-transformative, which negatively affected fair competition with the original copyright holder in the market.

This decision highlights that the Fair Use doctrine might serve as a legal basis for AI developers to train their models on copyrighted content without consent, but only within the limits of both the author's rights and the public interest. That said, not every use of existing works in the AI creation process constitutes copyright infringement, especially when the generated content results from inspiration rather than reproduction, leading to something new and innovative,[27] as stated: *"Copying a work is forbidden, whereas receiving inspiration is not only allowed, it is encouraged".*[28]

As the balance between the interests of authors and the public is sought, a key question arises of how copyright law should respond to AI-generated content.

[24] Congressional Research Service, "Generative Artificial Intelligence and Copyright Law", Legal Sidebar, 29 September 2023, p. 5.
[25] U.S. Copyright Office Fair Use Index, 2025, https://www.copyright.gov/fair-use/.
[26] Thomson Reuters v. Ross Intelligence, 1:20-cv-613-SB (D. Del., 2025).
[27] Yotam Werzansky-Orland, "The Market", International Journal of Business, Vol 5 (2024), p. 17, https://www.researchgate.net/publication/381566789_AI-Generated_Content_and_the_Question_of_Copyright.
[28] Ibid.

# V. Balancing the protection of AI-generated content with the promotion of human creativity and authors' interests

The copyrightability of AI-generated content does not depend solely on the application of copyright law. In truth, the distribution of copyright protection must also be fair and inclusive. The legislator cannot overly protect human authors while overlooking the potential of AI to support those with disabilities or creative limitations.[29]

AI was created to help humans with repetitive or complex tasks. Since not everyone has equal access to creative tools, why limit human creativity when AI can empower it? For example, if AI enables an expert with limited English proficiency to express their ideas and convey their message effectively, why should they not receive protection, not necessarily for the exact words suggested by AI, but for the original ideas and creative expression they shaped with its help. The use of AI should be encouraged to support the advancement of our economy and technology. Not only individual authors but also companies and business owners can benefit from AI to improve their services.[30] This progress should not be hindered by overly restrictive Copyright Law.

Nevertheless, this protection must be limited to preserve the integrity of human authorship. One way to achieve this is by granting copyright protection only to content that involves a certain degree of human contribution and reflects original human ideas. As Ryan Abbott, Professor of Law and Health Sciences at the University of Surrey (UK), explains: *"Allowing a person to be listed as an inventor for an AI-generated invention would not be unfair to an AI, which has no interest in being acknowledged, but allowing people to take credit for work they have not done would devalue human inventorship."* [31]

Purely AI-generated content, without human input, may lead to copyright infringement, especially when it closely resembles existing works. Even if AI developers have obtained permission to use authors' works to train their models, copyright cannot be granted to both the original work and the AI-generated work derived from it. Therefore, purely AI-generated content should not be eligible for copyright. However, this position has been challenged by the view that such content, despite being autonomously produced, should benefit from a shorter protection period to incentivize investment in AI research and innovation.

[29] United States Copyright Office, "Copyright and Artificial Intelligence", op.cit., p. 37.
[30] Yotam Werzansky-Orland, "The Market", op. cit., p. 14.
[31] Ryan Abbott, "The Artificial Inventor Project", op.cit.

# VI. Conclusion

Through this extensive legal analysis and various examples, AI-generated content can be copyrightable under the name of the corresponding AI user. Despite this possibility, the protection is limited to authors who have contributed their ideas and used AI merely as an assistive tool to offer a fair balance between fully original human work and the creative support provided by AI. While AI-generated content may be recognized, it must not infringe upon existing copyrighted works.

However, the analyses presented in this brief should be regarded as a preliminary contribution to future discussions surrounding copyright and AI-generated content. At present, Cambodian Copyright Law contains no provisions specifically addressing AI-generated content, and the legal interpretations based on foreign jurisprudence and practices may evolve or differ significantly from the actual development of Cambodia's digital society. Therefore, further discussion on this brief would be welcomed at any appropriate time.

# Section 03

# Digital Markets Law

# Tackling Subscription Trap in Cambodia's E-Commerce Sector: Issues of Automatic Renewals and Free Trial Conversions

**KOEUNG Kimhab**

[Senior Law Student at ELBBL of RULE, Junior IR Student at IISPP ]

As a research intern at the Center for Southeast Asian Studies, he mainly focuses on how the ASEAN Way influences regional responses to complex issues such as the Myanmar Crisis and the South China Sea dispute. Moreover, he has also earned several awards in debate contests including a Runner-Up in CAMDEBATE 2024, a Champion in YIGF 2024, and a Runner-Up in Cambodia Moot Court Competition 2025 conducted by the Extraordinary Chambers in the Court of Cambodia.

## I. Introduction

In recent years, Cambodia's digital economy has rapidly increased with a projected transaction value of $1.62 billion in 2023 and is expected to double to $2.87 billion by 2027.[1] The e-commerce sector alone contributed 6.68% to GDP in 2024 due to the rise of 19.7 million e-wallet accounts in 2023.[2] This shows the behavioral shifts of both consumers and business operators toward more convenient online transactions.[3] As e-commerce expands, purchasing subscription services, including streaming platforms and software services, has also gained popularity since it provides attractive free trials and special discounts for consumers.[4] However, these ideal offers can deceive consumers into recurring fees of high hidden costs once the trial ends afterwards.[5]

Despite various Prakas and laws, Cambodia's legal framework lacks specific requirements to prevent deceptive subscription practices, including the absence of mandatory disclosures regarding automatic renewals and post-trial charges, unclear standards for informed consumer consent, and inadequate sample cancellation mechanisms.[6] Without addressing these issues, consumers would face unfair practices and erode their trust in the digital marketplace. Therefore, this paper will analyze Cambodia's regulatory shortcomings related

[1] Marketing & Communications, "The Bold Rise of Cambodia Digital Economy Growth Today," Market Research Southeast Asia, April 20, 2025, https://marketresearchsoutheastasia.com/insights/articles/rise-cambodia-digital-economy-growth-today.
[2] "Cambodia Central Bank Enhances Digital Payment Systems Amid Growing Adoption: NBC Fiscal Stability Report 2023," Cambodia Investment Review, June 20, 2024, https://cambodiainvestmentreview.com/2024/06/20/cambodia-central-bank-enhances-digital-payment-systems-amid-growing-adoption-nbc-fiscal-stability-report-2023/.
[3] Supreme National Economic Council. Cambodia Digital Economy and Society Policy Framework 2021–2035. Phnom Penh: Royal Government of Cambodia, 2021, 4-5.
[4] Profitence Cambodia. E-Commerce in Cambodia: A Comprehensive Overview on the E-Commerce Landscape in Cambodia—Addressing Challenges, Initiatives and Opportunities (Phnom Penh: Profitence Cambodia), 2025, 5.
[5] Competition and Consumer Commission of Singapore, Subscription Trap Revised (Singapore: CCCS), 2020.
[6] ASEAN, ASEAN Guidelines on Consumer Protection in E-Commerce (ASEAN Secretariat), 2023, https://asean.org/wp-content/uploads/2023/03/ASEAN-Guidelines-on-Consumer-Impact-E-COMMERCE_V2-1.pdf,9-11.

to subscription traps, such as auto-renewals and hidden terms, while proposing several reforms based on three advanced best practices from the United States (**U.S.**), Singapore, and the European Union (**EU**).

# II. Cambodia's Inadequate Legal Response to Deceptive Digital Subscription

Cambodia's legal frameworks governing the E-Commerce sector remain evolving and overly general. For instance, this limitation can be seen in Article 27 of the Law on E-Commerce, which serves as the primary legal provision regulating Cambodia's digital marketplace. Although this provision requires online business operators to avoid misleading advertising, it still lacks mandatory conditions detailing proper refund procedures, clear disclosures of subscription terms, and simple cancellation processes, making it difficult for consumers to exit unwanted contracts.[7] Without proper legal reform, these problems will continuously undermine consumer autonomy, violate the principle of informed consent, and erode consumers' trust in future online businesses.[8]

## 1. Law on E-Commerce

Article 29 of this law outlines the obligations of sellers to provide "clear and intelligible information" regarding transactions. This includes mandatory disclosures about the seller's identity, address, communication channels, and transaction details such as payment methods and cancellation options.[9] However, there are some limitations within this provision in addressing subscription traps.

Firstly, it fails to require specific disclosure about subscription mechanisms since Article 29 does not require that business operators clarify whether a service is subscription-based or subject to auto-renewal, nor does it mention if a free trial will automatically convert to a paid plan. This oversight raises concerns about consumer protection, as many individuals would find themselves enrolled in recurring billing cycles without fully understanding the timing of such future charges. Moreover, the general reference to "terms, conditions, and costs" is unclear to ensure that businesses proactively provide necessary information to consumers for pre-contractual agreements.[10]

Secondly, this article does not define what constitutes "clear and intelligible". While it emphasizes that sellers must present information in an understandable manner, the lack of a clear definition allows for variability in how this requirement is met.[11] Therefore, sellers could somehow fulfill their obligations by presenting information in ways that are complex or buried within lengthy terms of service, making it harder for consumers to comprehend their commitments.

In addition, there are no procedural safeguards of consent or default settings. In Article 29, it does not address how consent to contractual terms must be obtained. It does not distinguish between affirmative (opt-in) consent and passive or presumed consent, nor does it prohibit the use of default

[7] Law on Electronic Commerce ("LOE"), No. NS/RKM/1119/017, 2019, Article 27.
[8] "E-Commerce and Digital Business in Cambodia: Legal Guidelines," Generis Online, accessed April 16, 2025, https://generisonline.com/e-commerce-and-digital-business-in-cambodia-legal-guidelines/.
[9] LOE, Article 29(1).
[10] Ibid., Article 29(1)(c).
[11] Ibid., Article 29.

checked boxes or other manipulative consent mechanisms.[12] Thus, the lack of specific procedures regarding the attainment of consent by distinguishing between valid and invalid forms of consent, businesses would exploit this ambiguity to secure consent through deceptive or other non-transparent methods, making the consumers prone to lose control over their financial engagements.[13]

## 2. Law on Consumer Protection

Initially, although Article 13 of this law prohibits misleading sales practices, it provides no definition or elaboration on what constitutes a "misleading act" in the context of digital commerce.[14] In other words, this article fails to define whether or not disclosing recurring billing constitutes a misleading act or pre-authorized payment following a trial period without a renewal notice falls within the scope of this provision.

Furthermore, despite Articles 23 and 27 requiring business operators to establish "information standards" by setting the minimum information standards for electronic commerc,e including, the disclosure of prices, terms, packaging, supply mechanisms, and digital formats,[15] there are still some limitations with its ability to fully cover subscription-based services.

Moreover, there is also an ambiguous regulatory body governing online subscription-based services since it grants authority to unspecified "competent regulators" without designating an independent agency to oversee digital subscription standard compliance.[16] For example, the National Committee for Consumer Protection (**NCCP**) can develop policies and consult on standards, but operates as an advisory body without independent enforcement powers.[17] Its ability to issue administrative sanctions or written warnings depends solely on requests from unspecified regulators or the Consumer Protection, Competition, and Fraud Repression Directorate-General (**CCF**),[18] thus limiting its autonomy and creating institutional diffusion.

Alternatively, articles 6 to 8 of this law allow consumers to form associations that are properly registered with the Ministry of Interior to represent and initiate lawsuits for those whose rights are infringed before the NCCP or the court and provide legal counselling services.[19] However, there are no active consumer protection associations operating in Cambodia.[20] For instance, the registered Cambodian Consumer Association lacks visibility and activity, and Cambodia has no affiliate in global networks like Consumers International as well.[21] Therefore, this uncertainty hinders consumers' ability to challenge deceptive subscription practices through legal action and seek compensation successfully.

## 3. Civil Code of Cambodia

Article 520 of this law governs sales following trial use, which is relevant to the free trial model commonly used in subscription services. It provides that a sale is concluded either (1) when the consumer explicitly agrees to the purchase during the trial period, or (2) when the consumer fails to express any objections and continues using the goods after the trial period has ended.[22] However, there are a few shortcomings within this provision when regulating the emerging issue of digital commerce.

Firstly, there is a presumption of consent from silence. Article 520(1) effectively permits the passive

[12] "Types of Consent," MineOS, accessed April 16, 2025, https://www.mineos.ai/articles/types-of-consent.
[13] European Data Protection Board. Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 2024.
[14] Law on Consumer Protection ("LOCP"), Article 13.
[15] Ibid., Article 23 & 27.
[16] Ibid.
[17] Sub-Decree on the Organization and Functioning of the National Committee for Consumer Protection, No. 135 ANKR.BK, Article 11.
[18] Ibid., Article 3.
[19] LOCP, Articles 6-8.
[20] Radio Free Asia, "Cambodia's Consumer NGO Is Failing to Protect Consumers," Last Modified 2024, https://www.rfa.org/english/commentaries/cambodia-ngo-consumer-01142024084815.html.
[21] Ibid.
[22] Civil Code of Cambodia ("CC"), Article 520.

acceptance of a contract through inaction known as browsewrap agreements.[23] This presumption has become dangerous in the context of digital commerce since many Cambodian consumers are not mainly tech-savvy and are unaware that the expiration of a free trial will trigger a paid subscription, particularly in the case where no prior reminder is made.[24] Hence, deeming the silence as an agreement would only facilitate the practices that exploit consumers rather than protecting them.

Secondly, this provision does not require any renewal notice or informed consent. In Article 52, it does not require the online seller to issue a reminder before the end of the trial period.[25] Nor does it require that the consumer affirmatively confirm their intention or actual willingness to continue using services on paid terms by ensuring they are fully aware of all terms and conditions, such as recurring expenses of subscription fees and a simple cancellation method.[26] Therefore, this legal vacuum would allow sellers to enrol consumers into unintended contracts with long-term debts based solely on unawareness of the continuity of usage or failure to opt out.

Lastly, this article prioritizes a traditional civil law presumption that assumes that by continuing to access services, consumers have read, understood, and accepted the full scope of the agreement, which implies their willful or informed consent. Nevertheless, these practices only work in traditional face-to-face contracts since users are often confronted with lengthy, complex, and unilateral terms of service that are non-negotiable in today's virtual environment.[27] These agreements generally prompt the users in ways that discourage thorough reading, hidden in hyperlinks, placed at the bottom of pages, or masked by design techniques, so-called "dark patterns" that deceive users into accepting without truly understanding what they are consenting to.[28]

## 4. Prakas on Unfair Practices in Business Related to Advertisements and Sales Promotions

This Ministry of Commerce's Prakas aims to tackle unfair business practices, particularly deceptive advertising and sales promotions that were previously underregulated under the Law on Consumer Protection.[29] It applies to all entities involved in marketing goods and services within Cambodia, including digital platforms, while prohibiting false or misleading claims, exaggerated superlatives like the "best," "only one," "number one," as well as the use of deceptive images or endorsements.[30] This regulation can somehow help address relevant subscription trap tactics like falsified free trials or hidden costs of auto-renewal. Therefore, any violations that fall under one of these dishonest practices would face capital fines of up to 50 million riels.[31]

Nevertheless, while this Prakas enhances protections against misleading promotional practices, it does not govern the contractual aspects of subscription services. It lacks provisions governing automatic renewals, mandatory disclosures about recurring charges, requirements for clear consumer consent, or procedures for simple cancellation processes. Hence, although the Prakas addresses the initial deceptive marketing tactics that draw consumers into subscription traps, it does not cover the contractual mechanisms that lock them in properly.

[23] Sergei Tokmakov, "The Evolution of Clickwrap, Browsewrap, and Sign-in Wrap Agreements," Terms.law, 2023, https://terms.law/2023/08/26/the-evolution-of-clickwrap-browsewrap-and-sign-in-wrap-agreements/.
[24] Profitence Cambodia. E-Commerce in Cambodia: A Comprehensive Overview on the E-Commerce Landscape in Cambodia—Addressing Challenges, Initiatives and Opportunities (Phnom Penh: Profitence Cambodia), 2025, 5.
[25] Subscriptions and Automatic Rollovers: Quick Guide. New Zealand Commerce Commission, 2018.
[26] Venable LLP, "Is a Checkbox Required to Obtain Consent to Subscription Programs?," Venable Insights, 2023, https://www.venable.com/insights/publications/2023/04/is-a-checkbox-required-to-obtain-consent-to.Venable LLP+1Venable LLP+1.
[27] "Payment Terms are a Non-negotiable Requirement for 8 out of 10 B2B Buyers, Hokodo Finds," Financial IT, 2024, https://financialit.net/news/e-payments/payment-terms-are-non-negotiable-requirement-8-out-10-b2b-buyers-hokodo-finds.
[28] Ashley & David, "How Companies Make It Hard for You to Cancel Online Subscriptions," RTÉ Brainstorm, 2024, https://www.rte.ie/brainstorm/2024/0509/1448035-dark-patterns-cancel-online-subscriptions/.RTÉ.
[29] Prakas on Unfair Practices In Business Related to Advertisements and Sales Promotions, No. 95 ANKR.BK, Article 1.
[30] Ibid., Articles 2 & 13.
[31] LOCP, Article 44.

# III. Bridging the Gaps in Cambodia's Legal Framework on Subscription Traps: Comparative Insights from the U.S., Singapore, and the EU

As Cambodia's legal framework on subscription traps remains outdated, it is important to explore and learn best practices from more advanced jurisdictions, particularly the U.S., Singapore, and the EU, since they provide models that are not only well-developed but also more suitable for Cambodia's legal and institutional context. As an ASEAN member, Singapore's jurisdiction emphasizes regional compatibility and shows how administrative enforcement can work effectively without complex legislation for Cambodia. Meanwhile, the EU's civil law system is closely aligned with Cambodia's French-based legal tradition, making its consumer protection laws easier to adapt from similar practices. For the U.S., despite having a different economic development level, it still provides strong examples of enforcement and business compliance that Cambodia can learn from to strengthen its weak regulatory mechanisms. Therefore, these three advanced jurisdictions offer more practical guidance for reform in five key areas, namely, the disclosure of terms, renewal notices, consent mechanisms, cancellation rights, and proper enforcement mechanisms.

## 1. The Need for Clear Disclosure of Subscription Terms

Under Article 29 of the Law on E-Commerce, essential information must always be presented in a "clear and intelligible" manner.[32] However, there is no express statutory provision that requires the disclosure of specific material terms governing recurring billing, automatic renewal, trial-to-paid conversion, or subscription duration. This uncertainty allows online businesses to insert financially binding terms into digital contracts without ensuring the consumer's full awareness of such obligations.

In contrast, the U.S Restore Online Shoppers' Confidence Act (**ROSCA**) requires that all sellers disclose "all material terms of the transactions, including recurring charges," clearly and conspicuously before obtaining the consumer's billing information.[33] Additionally, the Federal Trade Commission (**FTC**) has repeatedly interpreted this as requiring placement in close proximity to the order button, such as "order now" or "add to cart" buttons, in easy-read fonts and sizes, and not hidden in hyperlinked terms during the transaction flows.[34]

Regionally, the Singaporean 2020 Price Transparency Guidelines, despite being technically a non-binding framework, these domestic guidelines are treated as authoritative by the Competition and Consumer Commission of Singapore (**CCCS**) under the Consumer Protection (**Fair Trading**) Act (**CPFTA**), particularly concerning digital subscriptions. These guidelines specify that free trials must indicate the conversion terms, charges, and opt-out deadlines at the point of sign-up to ensure consumers' awareness.[35]

[32] LOE, Article 29.
[33] ROSCA, Pub. L. No. 111-345, § 3, 124 Stat. 3618 (2010).
[34] FTCA, 15 U.S.C. §§ 41–58 (2023).
[35] CCCS, CCCS Guidelines on Price Transparency, HR Section 3.4.11 (Singapore), 2020, https://www.cccs.gov.sg/-/media/custom/ccs/files/legislation/cpfta/price-transparency-guidelines-7-sept-20/cccs-guidelines-on-price-transparency_hr.ashx.

## 2. The Reform for Renewal Notice Requirement

Currently, there is no provision which requires advance notice of automatic renewals, even when the original contract was long-term or auto-renewing by default. The absence of such provisions would permit businesses to continue billing the consumers without any obligations to re-seek the consent or alert users beforehand of imminent charges.

Nevertheless, several states in the U.S., specifically California, with its Automatic Renewal Law, have required businesses to notify consumers between 15 to 45 days before renewal for contracts longer than one year.[36] This notice must contain a clear renewal date, price, and cancellation instructions.[37] This approach aims to preserve consumer autonomy and financial transparency at the point of contract continuation.

Meanwhile, in Singapore, while there is no statutory renewal notice obligation, there is still case law and administrative enforcement to fill such gaps. For instance, in *Fashion Interactive Pte Ltd v CCCS,* the failure to alert users of the expiration of a free trial and the start of paid billing was considered an unfair trade practice under the **CPFTA.**[38] Thus, this unfair practice was established when recurring charges were imposed without proper notice, particularly after a trial period, violating the principle of informed decision-making, even if the original terms technically included the renewal.[39]

## 3. The Mandatory Consent Attainment Mechanisms

Under the Civil Code of Cambodia, "silence" may constitute "acceptance", particularly where a business relationship suggests acquiescence or might be exposed to browsewrap agreements.[40] While this conventional business practice would be appropriate in traditional commerce, it does not suit best in the modern digital subscription models, where silence can result in binding financial burdens without clear consumer intent.

However, in the EU, under the General Data Protection Regulation (**GDPR**), consent must be "freely given, specific, informed and unambiguous," and must be expressed through a clear affirmative act.[41] Specifically, recital 32 rejects silence, inactivity, or pre-ticked boxes as valid forms of consent.[42] This framework not only informs EU data protection law but also influences broader contractual practices through the Consumer Rights Directive (**CRD**) and the Unfair Commercial Practices Directive (**UCPD**). Similarly, the U.S. ROSCA also provided that no recurring charge would be imposed without the consumer's express informed consent.[43] Therefore, FTC enforcement has made it clear that such consent must involve active user confirmation, typically through unchecked boxes or confirmation buttons proximate to the terms.[44]

## 4. Simple Cancellation Process

Since there are no legal obligations imposed on businesses to ensure that cancellation methods are accessible and as simple as the sign-up process, it allows service providers to use dark patterns to confuse, manipulate, or delay consumers from terminating subscriptions.

[36] California Business and Professions Code, §17602 (2023).
[37] Ibid.
[38] CCCS, E-Commerce Retailer Fashion Interactive Ordered to Cease Unfair Trade Practices and Stop Using "Subscription Traps", 2020, https://www.cccs.gov.sg/media-and-consultation/newsroom/media-releases/fashion-interactive-court-order-17-jan-2020.
[39] Ibid.
[40] CC, Article 520.
[41] GDPR, Recital 32.
[42] Ibid.
[43] ROSCA, § 4.
[44] FTCA, §§ 41–58.

In contrast, under Singapore CCCS's Price Transparency Guidelines and the CPFTA, traders must guarantee that cancellation is "as easy as subscriptions," available through the same digital channel, and can be made in minimal steps and a straightforward way.[45]

Similarly, the U.S. ROSCA requires business operators to provide consumers with a "simple mechanism to stop recurring charges".[46] With these requirements, the FTC has interpreted this as the cancellation must be possible through the original medium of subscription, such as the "click-to-cancel" rule, without unreasonable delay or procedural obstacles.[47] Likewise, the EU CRD provides 14 days of withdrawal right for distance contracts, including subscriptions, and requires that consumers can exercise that right without additional penalty or unreasonable burden.[48]

### 5. Independent Enforcement Oversight for Proper Refund Policies

As the only designated entity for consumer protection dispute resolution, the NCCP still lacks direct authority and relies solely on undefined "competent regulators", meaning the NCCP does not have investigatory independence, sanctioning authority, and digital complaint infrastructure where there is no mechanism to oversee compliance, initiate administrative sanctions, or provide timely compensations.[49]

However, in the U.S., there is an establishment of the FTC that possesses expansive powers in imposing civil penalties, seeking injunctive relief, and providing reasonable compensation for consumers affected by subscription traps.[50] Under the FTC's enforcement, there have been significant deterrent outcomes, including multimillion-dollar settlements and industry-wide compliance obligations across the whole nation.[51] For instance, in FTC v. ABCmouse, the Commission obtained a $10 million settlement over unlawful subscription practices, reinforcing the FTC's strong stance against deceptive auto-renewal schemes.[52]

Simultaneously, Singapore also offers a similarly effective model through the CCCS, which investigates unfair practices, imposes design changes, and maintains a public-facing complaint resolution portal.[53] Hence, these independent institutions can operate with clear statutory authority and handle online market disputes more effectively than Cambodia's NCCP.

# V. Conclusion

In conclusion, despite its fast-growing e-commerce sector, Cambodia's current laws fail to fully address digital issues like automatic renewals and free trial conversions since the existing legal frameworks are overly general and lack clarity on clear disclosures, deceptive practices, and informed consent processes by leaving consumers vulnerable to misleading subscription traps that can result in hidden fees and severe financial losses.

To maintain its e-commerce credibility and promote progressive growth, Cambodia must reform its laws to require clear subscription terms, explicit consumer consent, advance notifications for renewals, and easy cancellation processes based on stronger enforcement practices from the U.S.,

[45] CCCS, "CCCS Guidelines on Price Transparency," HR Section 3.1.6 (Singapore), 2020, https://www.cccs.gov.sg/-/media/custom/ccs/files/legislation/cpfta/price-transparency-guidelines-7-sept-20/cccs-guidelines-on-price-transparency_hr.ashx.
[46] ROSCA, § 4(3).
[47] The U.S. FTC. Negative Option Rule, 16 C.F.R. Part 425 (2024).
[48] EU CDR, Recital 40.
[49] Sub-Decree on the Organization and Functioning of the National Committee for Consumer Protection, No. 135 ANKR.BK, Article 11.
[50] The U.S. FTC. "Enforcement Authority." Last Modified May 2021. https://www.ftc.gov/about-ftc/mission/enforcement-authority.
[51] Ibid.
[52] FTC v. Age of Learning, INc & ABCmouse, No. 20-1032 (2021).
[53] CCCS, "Making Complaints.", Last Modified October 11, 2024. https://www.cccs.gov.sg/approach-cccs/making-complaints.

Singapore, and the EU. If these problems remain unchecked, they could deter e-commerce participation, discourage foreign investment, and harm the less tech-savvy consumers the hardest. Furthermore, further research should also focus on developing digital literacy programs to protect consumers from subscription traps in Cambodia. This future vision would allow consumers and stakeholders, like NGOs and policymakers, to find effective ways to empower online users and enhance their understanding of their rights and emerging issues in the digital field.

# Monetisation and randomness of the rewards mechanics – interpreting loot boxes as gambling?


## PRUM Sophеareach

[Legal associate at Sok Siphana Sethalay in association with Kinstellar Southeast Asia ]- KASFLY 2024

Currently an associate at a top-tier law firm's Licensing and Compliance Practice Group, Sophеareach has spent three years advising landmarks projects across digital business, investment, energy, and financial sectors. His expertise extends beyond practice, with published works spanning Trust, Advertising, FinTech, and Energy law. His legal writing has earned recognitions—capturing the Best Memorial Award at the prestigious Philip C. Jessup International Moot Court Competition (5th place globally among 500 teams in 2022) and claiming 1st place for Best Claimant Written Memorial at the National Commercial Arbitration Center Moot in 2024. He was also a KASFLY 2024 fellow.


# I. Introduction

By 2027, Cambodia's mobile game market is projected to grow significantly, with an anticipated increase in the mobile game consumer base to 3.1 million and a market volume reaching $47.57 million.[1] This is driven partly through the "microtransactions" business model, which is an umbrella term for the sale of in-game goods or other in-game advantages.[2] For this reason, more attention should be paid to "loot boxes," an in-game mechanism allowing players to purchase a randomized virtual box.[3] These systems vary in their accessibility, cost, reward, and content,[4] allowing variations that have a significant impact on players' gaming experiences and spending habits.[5] Because of that, players often invest money pursuing valuable and rare rewards, with young players being particularly the most affected by these effects.[6] This addictive nature is not a mere coincidence but rather a consequence of the deliberate introduction of predatory monetization schemes into the gaming industry,[7] which can be found in many high-profile game titles. The most extreme example is Diablo Immortal, with players spending over USD100k on loot boxes.[8]

[1] Prakash Jha, "Kingdom's mobile games revenue may reach $34.28M," Khmer Times, February 1, 2023, https://www.khmertimeskh.com/501230311/kingdoms-mobile-games-revenue-may-reach-34-28m/.
[2] Seppy Pour, "Experience of Legal Regulation of Loot boxes in Different Countries: a Comparative Analysis," Journal of Digital Technologies and Law, 2(2) (2024): p.347.
[3] Ibid.
[4] Ibid.
[5] Annette Cerulli-Harms et al, "Loot boxes in online games and their effect on consumers, in particular young consumers," Think Tank European Parliament Research, (2020): p.13.
[6] Leon Y. Xiao, "Drafting video game loot box regulation for dummies: a Chinese lesson," Information & Communications Technology Law 31, No.3, (2022):p.343.;Corey Bedford, "11-year-old boy spent £464 on game microtransactions and loot boxes," Leicestershire Live, December 5 2022, https://www.leicestermercury.co.uk/news/local-news/11-year-old-boy-spent-7877406; GMA Team, Doug Vollmayer and Elizabeth Schulze, "Parents share warning after son spends $4,000 playing video games," ABC News, April 4, 2024, https://abcnews.go.com/GMA/Family/parents-share-warning-after-son-spends-4000-playing/story?id=108845824.
[7] Daniel L. King, Paul H. Delfabbro, "Video Game Monetization (e.g., 'Loot Boxes'): a Blueprint for Practical Social Responsibility Measures," International Journal of Mental Health and Addiction, (2018):p.2.
[8] Tiago Svn, "It Costs $100K To Fully Gear Up One's 'Diablo Immortal' Character, Because Microtransactions," Cracked, June 06, 2022, https://www.cracked.com/article_34200_it-costs-100k-to-fully-gear-up-ones-diablo-immortal-character-because-microtransactions.html.

Due to psychological and financial risks, many maintain the belief that this monetization practice constitutes gambling. Therefore, this paper will explore the various arguments in favor of regulating loot boxes. An evaluation will be carried out to analyze the regulatory measures and outline a reform agenda informed by regulatory global responses to the issue. Particular attention will be paid to the most likely response to deal with loot boxes.

# II. Inadequacy of Existing Laws to Define the Classification of Loot Boxes and Ensure Consumer Protection

Before formulating the key principles and practices that should underpin a proposed regulatory approach to the issue, it is crucial to first identify and evaluate the diverse groups that are affected by the implementation of such legislation.

Relevantly, microtransactions have largely operated outside the regulatory controls and consumer safeguards that govern gambling activities.[9] Moreover, the lack of academic and legal consensus regarding its status poses a direct challenge to regulating in this field.[10] Many gambling regulators have debated whether loot boxes fall under existing national gambling laws, e.g., in Belgium[11] and the Netherlands,[12] whereas policymakers in countries have argued that they should be regulated as gambling through future amendments of law, e.g., in the UK,[13] USA,[14] and Australia.[15] Debates also continue regarding the extent to which regulating what could be considered a genuine commercial activity is appreciated in the name of consumer protection.[16]

## 1. Using Gambling Law to Analyze the So-Called "Illegal Wager" Activities

As a generally accepted definition, three elements must be satisfied for an activity to qualify as an illegal "wager": risking something of value (stake), on the occurrence of a chance event (chance), and for a potentially valuable price (price).[17]

Specifically, Cambodia prohibited online gambling in 2019 through a prime minister's order, while the *Suppression of Gambling Law.*[18] prohibits Cambodian citizens from gambling activities. However, these measures have not always been enforced to regulate video games.[19] From another standpoint, the Management of Commercial Gaming Law, if applied to this subject matter, may confront the same challenge that has emerged globally: the "price" element requirement.

[9] Daniel L. King, Paul H. Delfabbro, "Video Game Monetization (e.g., 'Loot Boxes'): a Blueprint for Practical Social Responsibility Measures," op.cit., p.2.
[10] Mark D. Driffiths, "Is The Buying of Loot Boxes In Video Games A Form of Gambling or Gaming?," Gaming Law Review 22, No. 1, (2018):p.54.
[11] VGFB, "Loot Boxes in Belgium,", VGFB.BE, https://vgfb.be/loot-boxes-in-belgium/#:~:text=This%2520means%2520that%2520players%2520in,private%2520internet%-2520connection%2520(VPN).
[12] Netherlands Gaming Authority, "Study into loot boxes. A treasure or a burden?," (Netherlands Gaming Authority, 2018), p.2., https://kansspelautoriteit.nl/publish/library/17/study_into_loot_boxes_-_a_treasure_or_a_burden_-_eng.pdf.
[13] John Woodhouse, "Loot boxes in video games," (UK Parliament, 2024), https://commonslibrary.parliament.uk/research-briefings/cbp-8498/.
[14] Josh Hawley, "A bill to regulate certain pay-to-win microtransactions and sales of loot boxes in interactive digital entertainment products, and for other purposes," (Congress,2019). s.1629, 116th, https://www.congress.gov/bill/116th-congress/senate-bill/1629.
[15] Parliament of the Commonwealth of Australia, "Gaming Micro-Transactions for Chance-Based Items" (Senate Environment and Communications References Committee, 2018), https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Gamingmicro-transactions
[16] Stephanie Derrington, Shaun Star, & Sarah J. Kelly, "The Case for Uniform Loot Box Regulation: A New Classification Typology and Reform Agenda," Journal of Gambling Issues 46, (2021):p.310.
[17] Stephanie Derrington, Shaun Star, & Sarah J. Kelly, "The Case for Uniform Loot Box Regulation: A New Classification Typology and Reform Agenda," op.cit., p.310.
[18] Royal Government of Cambodia, Law on the Suppression of Gambling, January 6, 1996.
[19] Teng Yalirozy, "Interior Ministry Orders Gambling Promotion Cessation: the Public Wants Real Action," Cambodianess, December 6, 2024, https://cambodianess.com/article/interior-ministry-orders-gambling-promotion-cessation-the-public-wants-real-action; Taing Rinith, "Unfettered online gambling sites targetting Cambodians,", Khmer Times, Decmber 6,

**Table 1:** Summary of Classifications of Loot Boxes: Gambling, Gaming, and Games of Chance

| | Definitions | Are loot boxes captured by the definition? |
|---|---|---|
| **Belgium** | "Games of chance" involve stakes that can be lost, with chance determining winners/gains.<br>(Gaming and Betting Act, 1999, art.2(1))[20] | Yes, loot boxes involve monetary transactions with chance and inherent risks. |
| **UK** | Games of chance for prizes (money or equivalent value).<br>(Gambling Act, 2005, s.6)[21] | Yes, if items can be "cashed in" or exchanged for money |
| **South Korea** | Obtaining monetary gain/loss through wagering property on chance-based activities. | No - under a separate regime requiring odds disclosure and spending limits |
| | (Supreme Court 2008. 10. 23. Sentence 2006 736 Judgment - Golf Gambling Case)[22] | |
| **Cambodia** | Games of chance are based on chance or a chance/skill combination. Games without payment requirements for the chance to win money or monetary prizes are not considered commercial gaming.<br>(Law on Management of Commercial Gaming, 2020)[23] | Unclear and unconfirmed - arguably fall within the "game of chance" definition, but the "price" element issue remains |

National Gambling Laws differ across countries, specifically, the various legal elements that must be satisfied. For example, under the UK Gambling Act, the "price" must be worth real-world money for the element to be satisfied;[24] in contrast, in Belgium, there is no "price" element per se, and the Belgian Gaming Act instead examines where there is a chance of winning or losses. The Belgian Gaming Commission found that the opening of the boxes in and of itself constituted the game element.[25] More restrictively, a price that does not hold value in real-world transactions is still considered a "win". Interestingly, Belgian law has never been amended to include loot boxes. However, the existing law can be interpreted to include boxes due to its drafting language. Thus, Belgium is currently the only jurisdiction in Europe to have outright banned the use of loot boxes.[26] Following a 2018 research report, game companies in Belgium voluntarily blocked loot box purchases in response to the study's findings.[27] In any event, under the Belgian Gaming Act, game companies would be held liable for criminal penalties for gambling within their games (without the necessary licenses).

Initially, the UK regulators proposed amending the UK Gambling Act to include loot boxes within its scope. However, the UK Government refused to do so in the absence of conclusive academic

[20] "Games of chance" involve a player staking any amount that can be lost to other players, the organizers, or a prize can be gained. Chance must determine the winner or distribute the gain.
[21] "Gaming & game of chance" means playing a game of chance for a prize. And "Prize" refers to money or its equivalent value and encompasses both prizes offered by an event organizer and the winnings obtained from money stakes.
[22] The Korean Criminal Code does not define "gambling," but the Korean Supreme Court has defined it as an act of obtaining monetary gain or loss through the wagering of property on a game or activity that relies on chance.
[23] "Game of chance" refers to commercial games outside licensed casinos, based solely on chance or a combination of chance and skill. "Commercial gaming" refers to games of chance operated for commercial purposes. Games that do not require payment for the chance to win money or something of monetary value are not considered commercial gaming.
[24] UK Gambling Commission, "Virtual Currencies, ESports and Social Gaming – Position Paper," (Gambling Commission, 2017), para.3.17, https://www.gamblingcommission.gov.uk/about-us/page/virtual-currencies-esports-and-social-gaming-discussion-paper.
[25] Peter Naessens, Secretariat of the Gaming Commission, "Research Report on Loot Boxes," (Belgian Gaming Commission, 2018), p.10, https://www.gamingcommission.be/sites/default/files/2021-08/onderzoeksrapport-loot-boxen-Engels-publicatie.pdf.
[26] Seppy Pour, "Experience of Legal Regulation of Loot boxes in Different Countries: a Comparative Analysis," op. cit., p. 354.
[27] Peter Naessens, Secretariat of the Gaming Commission, "Research Report on Loot Boxes," (Belgian Gaming Commission, 2018), https://www.gamingcommission.be/sites/default/files/2021-08/onderzoeksrapport-loot-boxen-Engels-publicatie.pdf; Peter Honer, "Limiting the loot box: overview and difficulties of a common EU response," Interactive Entertainment Law Review 4, No. 1, (2021):p.68.

evidence demonstrating a causal link.[28] Thus, current UK legislation classifies loot boxes as non-gambling if the virtual goods cannot be converted into cash. Though gambling regulators attempt to incorporate loot boxes into existing Gambling Laws, such assessments often fail for loot boxes whose rewards lack real-world value because the "price" element cannot be satisfied. They believed that the ability to convert in-game winnings into real-world currency is a crucial legal aspect of gambling.[29]

Another interesting fact to note is that the transactions made often lack direct financial returns, preventing players from recovering their spending. This distinction sets them apart from traditional gambling products, even though they share a similar structure.[30]

In the end, the question lingered: did the regulators' requirement for "real currency" truly align with its intended purpose, considering the potential harm it caused?

## 2. Loot Boxes May Be Governed by Unfair Commercial Acts and Practices Regulations

Having previously placed loot boxes within Gambling Law, it is time to investigate the scheme that both involves a state-centered approach and an industry-centered approach. The EU approach to applying EU Consumer Law to loot boxes is problematic for a few reasons.

The question becomes what exactly being sole and marketed means. The EU's *Modernization Directive.*[31] requires traders to provide information on "the main characteristics of the goods or services, to the extent appropriate to the medium and to the or service";[32] in a manner which is "clear and comprehensible."[33] For loot boxes, it is unclear which characteristic would need to be disclosed. If the "box" itself is considered as the service, it might involve mandatory disclosure of reveal odds, contents, or addiction warnings. Alternatively, if the mechanism of "randomization" as a whole is viewed as the service, describing potential rewards might be sufficient upon opening the box.[34]

Apart from the classification issue, there is a possibility that loot boxes, if caught under consumer law, could be in breach of the Unfair Commercial Practices Directive. Article 7 states that: a commercial practice is misleading if it withholds crucial information that consumers need to make informed decisions, potentially resulting in uninformed choices.[36] Indeed, proving causation may be difficult; the Directive is not infringed if, but for the act and practice, the average assumer would have made the transactional decision as he did.[37] This means the leading action or practice must play a role in changing the player's decision-making.[38] For example, the court determines that the average consumer may appreciate that loot boxes involve random chance, and would still have bought the loot box.[39]

[28] Department for Digital, Culture, Media & Sport, "Government response to the call for evidence on loot boxes in video games," (Government of UK, 2022), https://www.gov.uk/government/calls-for-evidence/loot-boxes-in-video-games-call-for-evidence/outcome/government-response-to-the-call-for-evidence-on-loot-boxes-in-video-games.
[29] Aaron Drummond, James D Sauer, "Video game loot boxes are psychologically akin to gambling," Nature Human Behaviour, Nature Human Behaviour," Nature Human Behaviour 2, (2018):p.530–532.
[30] Daniel L. King, Paul H. Delfabbro, "Video Game Monetization (e.g., 'Loot Boxes'): a Blueprint for Practical Social Responsibility Measures," op.cit., p.4.
[31] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of union consumer protection rules).
[32] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights,
amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, art.5(1)(a);
[33] Ibid., art.(1).
[34] Peter Honer, "Limiting the loot box: overview and difficulties of a common EU response," op. cit., p.68.
[35] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').
[36] Ibid., art.7.
[37] Office of Fair-Trading v Purely Creative Ltd [2011] EWHC 106 (Ch), [2011] CTLC 45 [71] (Briggs J).
[38] Leon Y. Xiao, "Drafting video game loot box regulation for dummies: a Chinese lesson," op. cit., p.348-349.
[39] Ibid.

In Cambodia, there are fundamental consumer rights concerned, particularly the right to disclosure and information,[40] the right to responsible marketing,[41] and the right to protection against misleading or deceptive acts.[42] Potential breaches of the 2019 Law on Consumer Protection may be made out concerning issues, for example:

**(1)** failure to disclose the probabilities of obtaining randomized rewards from loot boxes could be considered an unfair act;[43]

**(2)** implementation of mechanics that constantly change the probabilities of obtaining randomized rewards may be an unfair act involving services.[44]

**(3)** falsely advertising loot boxes as available for sale or at a limited discount only for a short time, then offering them at the same or even better discount later, maybe a misleading presentation;[45] and

**(4)** Paying content creators to create advertisements that highlight the "lucky" part of loot box openings, without indicating sponsored content by game developers, may be considered an unfair act.[46]

However, the possibility of the Consumer Protection Competition and Fraud Repression Directorate-General (**CCF**) regulating loot boxes as unfair is hypothetical, as the CCF has not yet used this authority to regulate in-game purchases.

One more issue is that additional alluring design features called "dark patterns" of loot boxes encourage players to repeatedly purchase them.[47] Regulations of the EU have not quite caught up with putting a stop to this practice. The only way the EU regulates dark patterns is by applying certain regulations indirectly.[48] These include unintuitive probabilities that lack visual cues that indicate the probability of success, unlike dice.[49] And, the probability fluctuates constantly based on purchase history[50] or player behavior data.[51] Besides confusing probabilities, loot boxes employ deceptive techniques such as (1) temporal and (2) monetary dark patterns to entice and mislead players.[52] One of the common ones is "grinding", a type of temporal dark pattern[53] that compels players to perform repetitive and mind-numbing tasks.[54] By deliberately making progress painfully slow and tedious, developers create artificial friction that pushes frustrated players toward purchasing loot boxes as an escape route to faster advancement.[55] For example, FIFA 22 demands that users seeking a single soccer player loot box containing the top players either buy it or spend 35 hours playing the game.[56] An equally common practice is "pay-to-win microtransactions",[57] a form of monetary dark pattern that exploits social or competitive nature to coerce players into making purchases they

[40] Royal Government of Cambodia, Law on Consumer Protection, November 2, 2019, chap.6.
[41] Ibid., art.4 and chap.7.
[42] Ibid, chap.4 and 5.
[43] Ibid, art. 9 - ""misleading consumers regarding the cost, price or quality of the goods or services" and "failure to present to consumers promises, expectations and relevant information"
[44] Ibid., art.11 – "prohibition on misleading acts concerning "characteristics" and "quality" of the services.
[45] Ibid., art.12 – "that goods or service is known for their price" and "that goods or service is in high demand".
[46] Ibid., art.9 – "act or representation such as advertising, sales promotion, and other indications".
[47] Cole Sharedelow, "Gamble-to-Win: Regulating Video Game Loot Boxes Under the FTC's Unfair and Deceptive Practices Doctrines,", Journal of Business and Technology Law 18, No. 2, (2023):p.339-342.
[48] Caroline Churchill, et al., "A regulatory deep dive into 'dark patterns'," (Womble Bond Dickinson (UK) LLP, 2023), p.6, https://www.womblebonddickinson.com/uk/insights/articles-and-briefings/reconnect-regulatory-deep-dive-dark-patterns.
[49] Leon Y. Xiao, Phillipo Newall, "Probability Disclosures are not Enough: Reducing Loot Box Reward Complexity as a Part of Ethical Video Game Design," Journal of Gambling Issues, (2022):p.3.
[50] See ibid., p.4.
[51] See Forbrukerrådet, "Insert Coin: How The Gaming Industry Exploits Consumers Using Loot Boxes," (Forbrukerrådet, 2022), p.16–17, https://www.forbrukerradet.no/siste-nytt/loot-boxes-how-the-gaming-industry-manipulates-and-exploits-consumers/.
[52] See ibid., p41–43.; See José P. Zagal et al., "Dark Patterns in the Design of Games," International Conference on Foundations of Digital Games 39, (2013):p.41-42.
[53] See ibid., p.41-42.
[54] See ibid., p.41.
[55] See ibid., p.41-42; see Forbrukerrådet, "Insert Coin: How the Gaming Industry Exploits Consumers Using Loot Boxes," op. cit., p.21.
[56] See ibid., p.34.
[57] See José P. Zagal et al., "Dark Patterns in the Design of Games," op. cit.,p.41–44.

they would not otherwise make.[58] For instance, Raid: Shadow Legends broadcasts global messages whenever players receive rare characters from loot boxes,[59] pressuring others to purchase similar rewards.[60] This deceptive practice, like many others, exploits cognitive biases to influence players' behavior and align them with social trends.[61]

# III. Potential Solutions – Looking Beyond Gambling Law Boundaries?

All loot boxes warrant regulatory oversight irrespective of whether their rewards hold real-world monetary value, though not necessarily under gambling per se. Perhaps interestingly, certain jurisdictions pursuing consumer protection approaches to loot box regulation have avoided gambling classification altogether, instead implementing broader measures.

## 1. Industry self-regulation as a preemptive response

The benefits of self-regulation purportedly derive from addressing specific concerns without governmental or regulatory interference in industry commercial operations.[62] For instance, both Apple and Google Play mandate that any game listed in their respective stores disclose the odds of winning each type of reward before purchases.[63] However, neither Apple nor Google independently verified the accuracy of disclosed probabilities under their self-regulatory policies,[64] instead relying solely on unscrutinized self-declarations from video game companies claiming compliance.[65] This hands-off approach is addressed in the UK, where the government concluded that it would be premature to consider legislative measures without first implementing enhanced industry-led protection.[66] Specifically, the Association for UK Interactive Entertainment published 11 principles and related guidance on loot boxes, endorsed by the UK government,[67] requiring companies to make probability disclosures and to provide robust parental control features.[68]

In a corresponding fashion, South Korea's self-regulation system, organized by the Korea Association of Game Industry (**K-GAMES**), offers a certification system. This system has an enforcement mechanism outlined in the self-regulatory code's *Enforcement Rules*.[69] Article 11 mandates monthly monitoring of compliance among the most popular games on each platform.[70] Article 12 established consequences for non-compliance. Upon initial breach, the company receives guidance to comply. A second violation triggers a formal warning, while a third infraction results in public announcement and decertification.[71]

At the same time, self-regulation often falls short because companies can simply choose to ignore voluntary measures. It is important not to overlook an example from K-GAMES showing imitations,

[58] See ibid., p.43.
[59] Forbrukerrådet, "Insert Coin: How the Gaming Industry Exploits Consumers Using Loot Boxes," op. cit., p.43.
[60] Ibid., p.44.
[61] Ibid.
[62] Stephanie Derrington, Shaun Star, Sarah J. Kelly, "The Case for Uniform Loot Box Regulation: A New Classification Typology and Reform Agenda," op. cit., p.309.
[63] Apple, "App store review guidelines," (Apple, 2019), https://developer.apple.com/app-store/review/guidelines/; Googleplay, "Monetization and ads," (Google, 2020), https://support.google.com/googleplay/android-developer/topic/9857752.
[64] Leon Y. Xiao, "Regulating loot boxes as gambling? Towards a combined legal and self-regulatory consumer protection approach", Interactive Entertainment Law Review 4, 1 (2021):p.40.
[65] Apple, "App store review guidelines," (Apple, 2019), https://developer.apple.com/app-store/review/guidelines/; Googleplay, "Monetization and ads," (Google, 2020), https://support.google.com/googleplay/android-developer/topic/9857752.
[66] Department for Digital, Culture, Media & Sport, "Government response to the call for evidence on loot boxes in video games," (Government of UK, 2022), para.243, https://www.gov.uk/government/calls-for-evidence/loot-boxes-in-video-games-call-for-evidence/outcome/government-response-to-the-call-for-evidence-on-loot-boxes-in-video-games.
[67] UK Interactive Entertainment, "New Principles and Guidance on Paid Loot Boxes," (Ukie, 2023), https://ukie.org.uk/news/new-loot-box-principles-agreed-by-industry.
[68] Ibid.
[69] Korea Association of Game Industry, Criteria on Implementation of Self-Regulation for Healthy Game Culture, July 1, 2018. ("Enforcement Rules of Self-regulation Code for Healthy Game Culture")
[70] Ibid.
[71] Ibid.

where certain non-compliant games continue to be popular among players. In such a case, legal sanctions may provide a more reliable solution; fines and injunctions may be the answer to continued non-compliant operations.[72]

## 2. Disclosure of the probabilities: a less restrictive alternative

Instead of regulating loot boxes as gambling, an alternative consumer protection measure has been proposed: requiring the disclosure of loot box probabilities. This measure would reveal how likely a player is to obtain randomized rewards.[73]

For example, the Republic of China's (**PRC**) Ministry of Culture has issued a Notice to adopt this measure by imposing legal obligations on game companies to publish probabilities.[74] Similarly, Taiwan's Consumer Protection Committee announced an amendment to the *Standard Contract for Online Game*[75] to require games offering lottery-winning products or activities shall disclose the percentage probability of winning each item on the homepage of the game's website, the game log-in page, or the "purchase page", and on the physical product packaging.[76] In addition, games shall include reminders stating that this is a chance-based product; the consumer is not guaranteed to obtain any specific product by virtue of purchasing or participating.

Worth mentioning for Cambodia that the potential consumer protection benefits can be improved by mandating probability disclosure not just game interface and official websites, but all player touchpoints- from pinned to the top of the game's social media posts, and included in video trailers and other advertisements of the game.[77]

Disclosure regulations should also address the timing of probability changes, particularly through one widely implemented method "pity-timers" that progressively increase rare reward odds.[78] These operate through two distinct approaches: table-based systems (switching to enhanced probability tables at intervals), e.g., using a standard rates table for pulls 1-10 and a high-rarity-only table for pull 11, and progressive systems (continuously increasing probabilities with each pull), e.g., where rare items might start at 1%, gradually increase to 50% after 80 attempts, and reach 100% guarantee after 99 attempts.[79] In practice, table-based systems are relatively straightforward to comply with, requiring disclosure of multiple probability tables when each table is used, and the exact probabilities for each reward on every table.[80] However, progressive systems are much more difficult to disclose properly because the probabilities continuously shift.

As a solution, there is a method to provide such disclosure by making calculations after every single loot box purchase to ensure that the disclosed probabilities remain accurate.[81] Future loot box probability disclosure regulation in Cambodia will inevitably require accurate disclosures and shall incorporate the element of "true, effective, verifiable, and substantive," while underlying pit-timer systems.

[72] Leon Y. Xiao, "Regulating loot boxes as gambling? Towards a combined legal and self-regulatory consumer protection approach", op. cit., p.40.
[73] Annette Cerulli-Harms et al, "Loot boxes in online games and their effect on consumers, in particular young consumers," op. cit., p. 42.
[74] Ministry of Culture of PRC, "Notice of the Ministry of Culture on Regulating the Operation of Online Games and Strengthening Concurrent and Ex-Post Supervisions," December 1, 2016, para.6.
[75] Consumer Protection Office (Taiwan), "Matters that should be recorded and should not be recorded in the finalized contracts of online game services," December 29, 2022. ("Mandatory and Prohibitory Provisions of Standard Contract for Online Game Connection Service").
[76] Ibid., art.6.
[77] Leon Y. Xiao, "Drafting video game loot box regulation for dummies: a Chinese lesson," op. cit., p.366.
[78] Ibid., p.370-371.
[79] Ibid.
[80] Ibid.
[81] Ibid.

## 3. Implementation of maximum spending limits: an interventionist approach

As mentioned earlier, the primary concern with loot boxes is overspending. Pre-commitment limit-setting allows users to voluntarily or compulsorily set a maximum amount they are willing to spend before engaging.[82] Once this limit is reached, a reminder message is sent, and a cooling-off period is initiated, preventing the player from spending further.[83]

Monthly maximum spending limits on online games have been imposed on players in South Korea and the PRC. In South Korea, these limits were applied to individuals under the age of 19 at ₩70,000 (approximately USD50) and to adults at ₩500,000 (approximately USD362).[84] The adult spending limit was set at an arbitrarily high threshold that would only prevent the most extreme cases of overspending. The PRC prohibits spending for minors under 8, allowing 16-year-olds to spend up to ¥200 (approximately USD28) and 16-18-year-olds to spend ¥400 (approximately USD56).[85] For our lesson, setting a maximum spending limit poses a challenge.

The crux of the matter lies in determining the appropriate amount of this limit. The regulator must assess what constitutes a fair and equitable amount of money to be spent on a game within a specific timeframe. This assessment is inherently arbitrary, as it demands the imposition of this limit on all players, regardless of their individual circumstances.[86]

## 4. Age ratings and parental control systems as a guide for purchasers and parents

Major self-regulatory gaming organizations, the North American Entertainment Software Rating Board (**ESRB**) and the European Pan-European Game Information (**PEGI**) label games with "In-Game Purchases (Includes Random Items)" (**ESRB**) and "Includes Paid Random Items" (**PEGI**).[87] The industry has adopted principles for loot box use, including prohibiting under-18 purchases without parental consent and requiring disclosure of loot box mechanisms for informed consumer choices.

But for Cambodia, we did not benefit from these established industry association structures, which may potentially adopt our rating system. As the models, the Australian Classification Board requires M ratings (unsuitable for children under 15) for games with chance-based in-game purchases and R18+ ratings (adult-only restrictions) for simulated gambling content such as casino-style games,[88] while South Korea's Games Rating Board (**GRAC**) has the discretionary certification authority to deny game approval.[89] In addition, the GRAC actively monitors the top 100 most popular games across platforms such as the App Store and Google Play Store for compliance and conducts continuous checks whenever new loot boxes are introduced through updates.[90] The GRAC also investigates reports from players and the media.[91]

[82] Leon Y. Xiao, "Regulating loot boxes as gambling? Towards a combined legal and self-regulatory consumer protection approach", Interactive Entertainment Law Review 4, No.1, (2021):p.40.
[83] Aaron Drummond, James D. Sauer and Lauren C. Hall, "Loot Box Limit-Setting: A Potential Policy to Protect Video Game Users with Gambling Problems?,' Addition, (2019):p.935.
[84] Kim & Chang, "Decision to Lift Monthly Spending Limits on Online Adult PC Games," (Kim&Chang, 2019), https://www.kimchang.com/jp/insights/detail.kc?sch_section=4&idx=19896; Leon Y. Xiao, "People's Republic of China Legal Update: The Notice on the Prevention of Online Gaming Addiction in Juveniles (Published October 25, 2019, Effective November 1, 2019)," Gaming Law Review 25, No. 9, (2021):p.53.
[85] National Press and Publication Administration of PRC, "Notice on the Prevention of Online Gaming Addiction in Juveniles," October 25, 2019; Melody Chan, "China's new gaming proposals to tackle overspending by children amid online outrage," CAN News, May 31, 2024, https://bit.ly/4kRyyl8.
[86] Leon Y. Xiao, "People's Republic of China Legal Update: The Notice on the Prevention of Online Gaming Addiction in Juveniles (Published October 25, 2019, Effective November 1, 2019)," op. cit., p.1-6.
[87] Stephanie Derrington, Shaun Star, Sarah J. Kelly, "The Case for Uniform Loot Box Regulation: A New Classification Typology and Reform Agenda," op. cit., p.315.[88] Ibid., p.370-371.
[88] Department of Infrastructure, Transport, Regional Development, Communication, Sport and the Arts, "New classifications for gambling-like content in video games," (Australia Government, 2024), https://www.classification.gov.au/classification-ratings/new-classifications-for-gambling-content-video-games
[89] Stephanie Derrington, Shaun Star, Sarah J. Kelly, "The Case for Uniform Loot Box Regulation: A New Classification Typology and Reform Agenda," op. cit., p.314.
[90] Leon Y. Xio, Solip Park, "Better Than Industry Self-regulation: Compliance of Mobile Games with Newly Adopted and Actively Enforced Loot Box Probability Disclosure Law in South Korea," OSF Preprints, (2024):p.17.
[91] Ibid.

This is a valuable model for Cambodia to emulate, given GRAC's proactive approach, combining regular monitoring of popular games with responsive investigations of specific titles following player complaints. We may also explore another viable option that involves enabling parents to disable in-game purchases and microtransactions, including paid loot boxes—through dedicated parental controls settings.

# IV. Conclusion

Loot boxes represent a profitable but problematic element in the gaming industry. What becomes increasingly apparent, however, is a cluster of legitimate concerns regarding transparency matters, the harmful effects on minors, and their troubling association with gambling mechanisms and addictive tendencies. Notwithstanding the debates and controversies, the loot box market continues expanding. This article has attempted to explore some of the issues faced by regulatory-level approaches to curbing the use of these predatory techniques. All we need is a recognition of the potential that existing measures emphasize the need for balancing risk mitigation with innovation. Consider that existing legal responses to loot boxes, whose effectiveness should be subject to proper assessment, must be critically examined and not regarded as definitive solutions that can eliminate all potential harms. It is important to consider which measurement would be most suitable for different age groups of players in the country, such as young children compared to adults. Ultimately, video games are not just for entertainment, and it is time to acknowledge this.

# From Silence to Consent? A Legal Analysis of Advertising Communications: A Comparison of the Cambodian, Singaporean and European Frameworks

**HENG Chandarith**

[Senior law student at ELBBL of RULE]

He has served as an advisor for international moot courts and interned at Davies SM Attorneys-at-Law, contributing to research on corporate, AML, gambling, IP, and tax law. His work bridges law, policy, and business, aiming to shape Cambodia's legal future.

## I. Introduction

Consent plays a fundamental role in regulating both physical and digital interactions, particularly in determining how businesses communicate with customers, such as sending product advertisements or collecting personal data for marketing.[1] When it comes to digitalization, Cambodian laws are still developing, creating ambiguity in key areas such as opt-in and opt-out mechanisms for marketing communications. According to Article 30 of E-Commerce Law, the concept of consent is based on an opt-out by stating that senders of unsolicited commercial messages *"shall provide the consumer with a clearly specified and easily activated option to reject the unsolicited commercial communication."* However, it does not specify which types of communications do not require prior consent. Besides, this E-Commerce Law lacks key procedural guidelines on how consent should be obtained, revoked, or transferred in the context of electronic communications. This ambiguity creates legal uncertainty, exposing consumers to privacy risks while leaving businesses unsure how to comply. The distinction between opt-in, which requires explicit permission, and opt-out, which assumes consent unless refused,[2] is important in defining legal boundaries for consent.

[1] Peter P. Swire and Kenneth A. Bamberger, "The Danger of Mandatory Opt-In for Cookie Notices," Washington University Law Review 91, no. 4 (2014):1461-1503, p1463
[2] Monica Senor, "Opt-in, Opt-out and ADV Communications." Medialaws, January 18, 2012, https://www.medialaws.eu/opt-in-opt-out-and-adv-communications/.

This law brief explores current legal frameworks on digital consent under Cambodian laws, by focusing on gaps related to consent mechanisms. By comparing European and Singaporean approaches to opt-in and opt-out standards, as they have implemented comprehensive regulations,[3] the brief identifies best practices and offers recommendations to strengthen consumer protection and legal clarity in Cambodia's digital landscape.

# II. The State of Digital Consent in Cambodian Law: Gaps and Challenges

In Cambodia, there is currently no comprehensive law governing digital consent or data protection. Therefore, any legal assessment must draw from existing legal instruments, including the Civil Code, E-commerce, Telecommunication, and Consumer Protection Law, that touch upon the notion of consent, either directly or by implication.

## 1. Civil Code and Contractual Consent

From a contractual standpoint, the Civil Code recognizes that, for a contract to be binding, consent must be established before performance.[4] This demonstrates that the Code recognizes the significance of intent in forming contracts. On the other hand, if an obligation arises from a unilateral legal act, it must result from a clear expression of intent and the exercise of a right granted by contract or legal provisions.[5] Therefore, the Code explicitly states that no contract can exist without consent.

While the contract requires the offer and acceptance, in digital consent, one common issue is bundled consent, whereby a party is compelled to agree to a wide range of unrelated purposes in a single agreement.[6] Although it is an opt-in, the user did not have a chance to review and reject some of the cookies,[7] and it is presumed not to be freely given since individuals cannot control which elements they accept or refuse.[8]

## 2. E-commerce Law and Unsolicited Communications

Meanwhile, the rise of digital commerce has led to an increase in marketing communications. Thus, the E-commerce Law has addressed this concern, allowing the business to exercise the practice of unsolicited communication provided that they provide a clear and easily activated opt-out option to the individuals.[9] The provision did mention the term "clearly specified and easily activated". In practice, this is unclear and allows businesses to claim compliance, such as placing opt-out mechanisms in a small box and putting a hidden link near it, leading to them to a scam website.[10] In some cases, businesses may not even provide an opt-out option at all,[11] leaving consumers with many unsolicited communications.

[3] Lisbeth Lanvers Shah, "Data Regulation – Singapore." DS Avocats, October 26, 2023. https://www.dsavocats.com/en/data-regulation-singapour/.
[4] Cambodia Civil Code, Royal Kram No. NS/RKM/1207/030, promulgated on December 09, 2007 ("Civil code"), Article 336.
[5] Civil code, Article 312.
[6] Information and Privacy Commission NSW, Fact Sheet – Consent, 2023, p2.
[7] Batja Huisman, "Types of Consent: Understanding the Key Differences," MineOS, September 05 2022, https://www.mineos.ai/articles/types-of-consent..
[8] European Union, General Data Protection Regulation ("GDPR"), Regulation (EU) 2016/679, Recital 43.
[9] Law on E-commerce, Royal Kram No. NS/RKM/1119/017, promulgated on November 02, 2019 ("E-Commerce Law"), Article 30.
[10] Hongseng Rov, "Warning Issued Over SMS Phishing Scams" Kiripost, June 23 2023. https://kiripost.com/stories/warning-issued-over-sms-phishing-scams.
[11] Kuch Sikol, "Concerns Mount Over Growing Number of Spam SMSs." Kiripost, August 14, 2024. https://kiripost.com/stories/concerns-mount-over-growing-number-of-spam-smss.

Additionally, businesses must disclose essential details in Khmer, including their legal names, business address, contact information, and terms related to cancellations and withdrawals.[12] These terms are important because they directly affect the consumer's right to opt out of consent.[13] Despite legal requirements, many businesses conceal key details, leaving consumers unable to identify them or what is behind the communication.[14]

Besides, the E-Commerce Law fails to specify which types of communication require consent.[15] Without clear criteria distinguishing between opt-in and opt-out communications, it becomes difficult to determine when a message constitutes unsolicited communication. As a result, this leaves a grey area, making it hard to define whether one communication amounts to valid consent.

## 3. Telecommunications Law and Spam Risks

Promulgated in 2015, the Telecommunication Law primarily focuses on ensuring privacy, security, and safety for telecommunications users.[16] However, this law appears not to address the matter of consent.

A key weakness of the law is its failure to regulate the use of consumer data for marketing purposes. There are no specific data breach provisions, consent requirements, or restrictions on data transfers, allowing telecom operators to share subscriber information without clear consumer safeguards.[17]

## 4. Consumer Protection Law and Withdrawal of Consent

Under Consumer Protection Law, consumers are granted certain rights, including the right to information and protection from fraudulent or misleading advertisements,[18] ensuring that consumers can make informed decisions. In another aspect, consumers still can terminate the contract, particularly in situations where they may have been pressured into making a decision or where they change their mind about a purchase.[19] The Ministry of Commerce has further strengthened these protections through a Prakas introducing a cooling-off period, which permits consumers to cancel certain transactions within seven days.[20]

However, these protections primarily apply to sales transactions.[21] and do not extend to the regulation of consent for digital communications. Once a consumer gives consent to receive promotional materials, there is no precise legal mechanism that allows them to easily withdraw that consent.[22] This legal gap leaves consumers exposed to persistent and unwanted messaging, while businesses operate without clear boundaries on the duration and revocability of consent.

[12] E-Comerce Law, Article 29.
[13] European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679, May 4, 2020. p33.
[14] Kuch Sikol, "Concerns Mount Over Growing Number of Spam SMSs." op.cit, p3.
[15] E-Comerce Law, Article 30.
[16] Telecommunication Law, Article 1.
[17] Jay Cohen, Chandavya Ing, "Cambodia", in Regional guide to Cybersecurity and Data Protection in Mainland Southeast Asia (Tilleke & Gibbins, 2024), p5.
[18] Consumer Protection Law, Royal Kram No. NS/RKM/1119/016, promulgated on November 02, 2019, Article 4(6).
[19] MOC Prakas No.0113 on the Cooling-Off, Article 1.
[20] Ibid, Article 6.
[21] MOC Prakas No.0113 on the Cooling-Off, Article 2.
[22] DLA Piper, "Electronic Marketing in Cambodia." Data Protection Laws of the World. Last modified January 20, 2025. https://www.dlapiperdataprotection.com/?t=electronic-marketing&c=KH#insight

# III. Benchmarking Consent Regimes: Lessons for Cambodia from European and Singaporean Implementation

Cambodia's reform of its legal framework on consent in advertising communications should take a holistic approach, carefully balancing international best practices with the country's unique digital development path.[23] As we cannot adopt a one-size-fits-all approach, it should be varied depending on the forms of digital communication, balancing both consumer protection and business. This Brief compares the legal frameworks of the European Union and Singapore as comparison.

The EU prioritizes comprehensive data protection,[24] by mandating explicit, informed, and voluntary consent for data processing, and strengthening transparency and accountability.[25] It also enforces granular consent, allowing users to selectively choose data processing.[26] Additionally, the ePrivacy Directive further regulates digital marketing by requiring consent for online like cookies, reinforcing user privacy.[27]

Besides, Singapore's framework adopts a more pragmatic model, focusing on balancing business interests and individual privacy rights.[28] It mandates consent for data collection and use but allows for certain exceptions. Besides, Singapore also offers a good model for regulating unsolicited communication,[29] and this allows consumers to control unwanted messages. By drawing from the EU and Singapore, Cambodia can develop effective, context-appropriate reforms to strengthen consent and protect consumers in digital marketing.

## 1. Clear Guidelines for Opt-Out Consent in E-Commerce Law

Under the Privacy and Electronic Communications Regulations, only the commercial marketing of products and services is allowed to be sent with an opt-out mechanism.[30] Before sending, businesses are required to arrange marketing plans.[31] For example, whether it involves sensitive or child data or not, all communications focus exclusively on the commercial promotion of products or services. Besides, the consumer shall be informed how and why their information is taken for the communication, either by third parties or from publicly available information.[32]

In addition, under Articles 13 and 14, the General Data Protection Regulation (**GDPR**) imposes a duty of transparency, requiring businesses to disclose if they intend to retain and se this data for

[23] Royal Government of Cambodia. Cambodia Digital Government Policy 2022–2035, Preamble, p1.
[24] Ben Wolford, "What Is GDPR, the EU's New Data Protection Law?" GDPR.eu, n.d., https://gdpr.eu/what-is-gdpr/.
[25] GDPR, Article5-7.
[26] European Data Protection Board. Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms. April 17, 2024, p3.1
[27] Cookie Information. "What Is the ePrivacy Directive?" https://cookieinformation.com/what-is-the-eprivacy-directive/#:~:text=The%20ePrivacy%20Directive%2C%20also%20known,-data%20privacy%20in%20electronic%20communications.[17] Jay Cohen, Chandavya Ing, "Cambodia", in Regional guide to Cybersecurity and Data Protection in Mainland Southeast Asia (Tilleke & Gibbins, 2024), p5.
[28] Rob Bratby, "Singapore Takes Business-Friendly Approach in Data Protection Guidelines." ZDNet, September 30,2013, https://www.zdnet.com/article/singapore-takes-business-friendly-approach-in-data-protection-guidelines/.
[29] DLA Piper, "Electronic Marketing in Singapore," op.cit, p3.
[30] Information Commissioner's Office("ICO"), "Identify Direct Marketing", last modified March 28, 2023, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/identify-direct-marketing/.
[31] ICO, "An Introduction to Direct Marketing –A Step-by-Step Guide for Your Small Business" last modified April 10, 2025, https://ico.org.uk/for-organisations/advice-for-small-organisations/an-introduction-to-direct-marketing-a-step-by-step-guide-for-your-small-business/.
[32] Ibid.

future marketing.[33] Moreover, businesses must provide minimum information, name and contact details, purpose, and duration of processing.[34] At the end of the day, the individuals always have the right to object to the use of their data for direct marketing,[35] regardless of the lawful basis for data processing.[36]

Similarly, under the Personal Data Protection Act of Singapore (**PDPA**), certain types of commercial communications are classified as "specified messages" that can be sent without prior consent if their purpose is to commercially advertise, promote goods, services, or investment opportunities.[37] However, businesses must carefully evaluate whether they meet the eligibility criteria for sending such communications by considering four key factors.[38] (1) data minimization, collecting only essential information; (2) purpose limitation, clearly defining the communication's objective; (3) recipient benefit, ensuring value to consumers; and (4) proportionality, evaluating appropriateness in context. Importantly, even for these permitted communications, businesses must always provide a mechanism to withdraw consent and must honor any opt-out requests immediately.[39]

Opt-out mechanisms have put the burden on consumers as they must protect themselves from unwanted communications, while allowing businesses to presume consent from silence or inaction. Notably, Singapore has implemented a national Do Not Call (**DNC**) Registry,[40] allowing individuals to block promotional messages via SMS, phone calls, or fax by registering with this institution,[41] as the Personal Data Protection Commission (**PDPC**) did not see the opt out option as a good choice for obtaining consent for the receipt of direct marketing messages.[42] This model demonstrates how opt-in requirements create stronger accountability for businesses engaging in direct marketing.

To address ambiguity in the E-commerce Law and spam issues under the Telecommunication Law, Cambodia needs clearer rules and practical enforcement. Singapore's model offers useful guidance factors that distinguish between different types of marketing communications, and consideration of the plan before sending. Opt-out communication should only apply to socially acceptable ads like product updates,[43] with easy unsubscribe options. In contrast, unsolicited messages like casino ads should be restricted. Businesses must identify themselves clearly and stop all marketing once consent is withdrawn. To ensure compliance, Cambodia should establish a national opt-out system, like Singapore's DNC Registry. This system would let individuals block unsolicited messages, and businesses must check the DNC list before contacting them.

## 2. Opt-In Requirement for Specific Marketing Communications

Under EU laws, they establish a strict opt-in model for most forms of direct marketing. When it comes to electronic communication, the ePrivacy Directive (**ePD**), as a lex specialis to the GDPR,[44] mandates prior consent for automated calls, faxes, and electronic mail used for direct marketing.[45] This requirement is reinforced by Articles 6 and 7 of GDPR, which require prior consent from the individuals, and those consents shall be freely given, specific, informed, and unambiguous, and clear

[33] ICO, "Collect Information and Generate Leads," Direct Marketing Guidance, n.d., https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/collect-information-and-generate-leads/.
[34] GDPR, Article 13.
[35] ICO, "Direct Marketing and Regulatory Communications," last modified March 28, 2023, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-and-regulatory-communications/.
[36] GDPR, Article 14(2); ICO, "A Guide to Lawful Basis.", n.d, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/.
[37] PDPA, Section 37.
[38] PDPC, Advisory Guidelines on Requiring Consent for Marketing Purposes, May 8, 2015, p7.
[39] PDPA, Section 47.
[40] PDPC, Advisory Guidelines on the Application of the PDPA to Election Activities, July 28, 2023, p15.
[41] Do Not Call Registry. Infocomm Media Development Authority. n.d., https://www.dnc.gov.sg/index.html.
[42] PDPC, Advisory Guidelines on Key Concepts in the PDPA, May 16 2022, p51.
[43] GDPR Register. "Direct Marketing Rules and Exceptions.", November 2, 2022. https://www.gdprregister.eu/gdpr/direct-marketing-rules-and-exceptions/.
[44] GDPR, Article 95.
[45] ePD, Article 13(1).

affirmative action to be a valid consent.[46] Notwithstanding, Article 13(2) of the ePD permits businesses to send direct marketing messages to existing customers without prior consent if their contact details were obtained during a sale, so-called "soft opt-in".

Moreover, if the advertisements related to the children's data require parental consent under Article 8 of GDPR and sensitive data, such as healthcare product offers or financial services,[47] the communication shall demand explicit consent unless another legal basis applies, for example, processing necessary for compliance with a legal obligation or to protect vital interests.[48] Furthermore, the GDPR recognizes consent only when it is given freely for processing,[49] meaning the consumer chooses to be processed. Therefore, businesses cannot put the pre-condition such as agreeing to all[50] or using pre-ticked boxes.[51] This approach aims that each processing requires a separate opt-in, and consumers can reject what they do not consider essential for them.

Besides, data subjects have an absolute right to object to direct marketing,[52] and the businesses shall immediately cease processing upon request. Thus, even if a business argues legitimate interest for marketing, the data subject's objection always overrides it.[53] To comply with this regulation, businesses must identify themselves or the sender on whose behalf they are marketing, ensuring transparency to the customer.[54] Additionally, they must provide easy and accessible opt-out mechanisms, allowing individuals to withdraw consent.[55]

On the other hand, similar to the GDPR, it requires that consent be informed and voluntarily given.[56] The PDPA provides a pragmatic model suitable for emerging economies.[57] In certain cases, the PDPC requires businesses to obtain consent before sending marketing messages, especially those offering benefits like discounts or special deals.[58] If a business wishes to provide such offers, prior consent may be necessary. Additionally, businesses must secure explicit consent before contacting individuals registered with the DNC. Overall, while the requirement for prior consent before sending marketing communications is similar, the EU's regulations offer a thorough model for consent standards, while Singapore shows how these concepts can be thoughtfully adjusted to suit various market conditions.

For Cambodia, it should adopt stricter requirements for certain types of communications, drawing from the standards set by the GDPR and ePD to define when prior consent is needed for child and sensitive marketing via email, SMS, or social media. Hence, there should be additional regulations to supplement the Civil Code for addressing this. Alongside this requirement, businesses must provide a clear and easily accessible option for withdrawing consent, for instance, by putting an unsubscribe button.[59]

[46] GDPR, Article 4(11).
[47] GDPR, Article 9.
[48] GDPR, Article 6.
[49] GDPR-Info.eu. "Consent." GDPR Info. May 15, 2025. https://gdpr-info.eu/issues/consent/.
[50] GDPR, Article 7.
[51] CookieYes, "Does a Pre-Ticked Box Count as Consent?," n.d., https://www.cookieyes.com/knowledge-base/gdpr/does-a-pre-ticked-box-count-as-consent/.
[52] Article 21(2), (3), GDPR.
[53] GDPR-Info.eu. "Email Marketing under GDPR.", op.cit, p6.
[54] GDPR-Info.eu. "Email Marketing under GDPR.", op.cit, p6.
[55] ePD, Article 13(4).
[56] PDPA, Section 19.
[57] Danish Consumer Ombudsman, Guidance on Unsolicited Communications with Specific Customers, December 2018, p219.
[58] PDPC, Advisory Guidelines on Requiring Consent for Marketing Purposes, op.cit, p5.
[59] Astird Braken, "Legal Pitfalls Around Unsubscribing from Newsletters," Certified Senders Alliance, April 26, 2023, https://certified-senders.org/blog/legal-pitfalls-around-unsubscribing-from-newsletters/.

Furthermore, in addressing the issue of bundled consent noted earlier, it must be explicitly prohibited as it violates the principle of freely given consent. Instead, Cambodian regulations should require different consent; this would allow individuals to selectively agree to certain categories of communications or data uses while rejecting others.

### 3. Duration of Consent and Renewals

Neither GDPR nor ePD sets a fixed expiration period for the validity of consent. However, from the viewpoint of the Information Commissioner's Office, it depends on whether it is still aligned with consumer expectations.[60] For example, if consent was made to receive a particular promotional campaign, which was only anticipated to last a short period.

Similarly, under the PDPA,[61] data retention is deemed expired when it is no longer necessary. This is assessed by whether the data no longer serves its original purpose and is not required for legal or business reasons.[62] If consent is no longer valid or the data is no longer needed for its original purpose, the business must cease its use and delete it. Furthermore, the business cannot rely on prior consent for unrelated purposes or treat it as implied consent.[63] For example, subscribing to a newsletter does not permit businesses to send other promotional materials. This violates the principle of limitation, and the business shall notify the data subject to allow the use or disclosure of personal data for other purposes.[64]

The Cambodian Consumer Protection Law lacks clear mechanisms for withdrawing or expiring consent in ongoing marketing campaigns. Reflecting the accountability principles embedded in both the GDPR and the PDPA,[65] consent cannot be indefinite, and if the business wants to keep sending messages after consent expires, it must ask for consent again.

Lastly, following best practices, Cambodia should introduce a statutory requirement for commercial data controllers to retain and document all evidence of consent. These records should include the date, method, and scope of the consent obtained by the business for their processing.

# IV. Conclusion

Cambodia's current legal framework fails to adequately regulate consent in marketing communications, leaving consumers vulnerable in the digital era. The lack of consent standards and weak enforcement mechanisms has created an environment in which consumer rights are poorly protected in marketing. Therefore, Cambodia should reform its approach to consent by adopting robust, enforceable protections aligned with benchmarks like the GDPR and the PDPA. While this brief highlights the structural gaps in Cambodia's consent regime in the view of the legal landscape, it does not explore the socioeconomic or cultural factors that may influence compliance with stricter regulations, such as digital literacy rates or business resistance to change. Although beyond the scope of this brief, these factors could shape the practical implementation of future reforms and merit further examination.

[60] ICO, Direct Marketing Guidance, March 6, 2018, p33.
[61] PDPA, Section 25.
[62] PDPC, Advisory Guidelines on Key Concepts in the PDPA, op.cit 7, p117.
[63] PDPA, Section 15.
[64] PDPA, Section 16.
[65] OneTrust DataGuidance and Rajah & Tann Asia, GDPR v. Singapore's PDPA, n.d., p33

To further research, it should raise the issue to critically examine the enforcement mechanisms. Research could assess the institutional feasibility of criminalizing businesses that unilaterally process the data without consent, and draw lessons from the challenges faced by similar agencies in developing economies regarding the criminalization. This research should assess whether Cambodia's legal framework can support liability offenses for businesses that violate consent requirements, while balancing with economic development.

# Legal Challenges on Consumer Protection in E-Sport Sector in Cambodia: Challenges and Solutions


## SIM Sokchantepy

[Junior associate at Soksipha Sethalay & Associates]

She works within the Corporate and Commercial Department. She has hands-on experience providing legal advice and support to both local and international clients, particularly in matters involving business transactions, contract review, and regulatory compliance. Tepy holds a Bachelor of Law from RULE.


# I. Introduction

In the past, Electronic sports ("**E-sports**") was something only a few people in Cambodia knew or heard about. But Currently, with the advent of the electronic age, Esports have become a part of the Cambodian identity.[1] Despite rapid rise, E-sports in Cambodia remain largely unregulated and misunderstood within existing legal frameworks. E-sports is intentionally referred to as any form of video gaming, competitive or organized digital gameplay involving individual players or teams using electronic devices.[2]

Insight shows that video games influence children's physical health, mental health, social behaviours, and cognitive development.[3] Over 70% of gamers aged between 8-15 said they play video games most days or every day. That holds true regardless of age or gender, with 64% of girl saying that gaming is a regular part of their routine.[4] With this, the E-ports demographic skews young, making minor a significant portion of the player base. This group is uniquely vulnerable to a range of online harms, from exposure to inappropriate content to financial exploitation and data misuse. Given that the current legal protections are wholly inadequate for the online environment. Proposal for a strategic and sustainable legal framework that supports the responsible

[1] Jose Rodriguez T. Senase, Khmer Time, "Lack of inclusiveness: A challenge to the growth of Esports", october 5 2020, https://www.khmertimeskh.com/50769869/lack-of-inclusiveness-a-challenge-to-the-growth-of-esports/.
[2] DLA, PIPER, "E-Sports Law around the world", https://passle-net.s3.amazonaws.com/Passle/5c61908fabdfe912ccc9057c/MediaLibrary/Document/2020-04-14-17-51-57-575-A03400_EsportsoftheWorld_Booklet_Report_V71.pdf.
[3] Daniel Alanko, National centre of biotechnology information, "The Health Effects of Video Games in Children and Adolescents", January 2023, https://pubmed.ncbi.nlm.nih.gov/36587018/.
[4] Katie Gisenan, "The next gen: getting to know kid's relationship with video games", https://www.gwi.com/blog/kids-relationship-with-video-games.

growth of the E-sports industry while safeguarding the rights and well-being of Cambodian consumers, especially minors. And ensure that the digital economy advances in an ethical and inclusive manner is needed.

Likewise, this brief aims to provide a comprehensive examination of the legal vacuum surrounding consumer protection in Cambodia's E-sports industry. It highlights the inadequacies in current laws and regulations, focusing specifically on the Law on Consumer Protection,[5] Civil Code,[6] Criminal code, the urgent need for Prakas on age verification and content classification[7] and the lack of data privacy protections.

# II. The Urgent Need of Prakas on Age Verification and Content Classifitcation

Article 17 of Cambodia's Civil Code (**CC**) defines minors to any person under the act of eighteen.[8] In addition, the Article 18 of CC, mentioned that an act conducted by minors without the consent of their parental power holder or guardian may be rescinded.[9] Nevertheless, these protections are not working well in digital environments. A child can access games rated for mature audiences simply by clicking "Yes" to a prompt.[10] They can accept complex terms of service or interact with strangers online with minimal friction. These design flows allow minors to be exposed to graphic content, violence, or inappropriate chat rooms. They can agree to complicated terms of service or join online chats with strangers, without realizing what they are agreeing to.[11] These weak protections allow children to be exposed to harmful content such as violence, graphic images, or inappropriate conversation. Currently, Cambodian parents are expected to take full responsibility for monitoring their children's online activity. But in reality, many parents do not fully understand the technology their children use, making it hard to protect them. The companies that create and profit from games should also take responsibility for keeping young users safe.[12]

To protect minors from liability related to breaching their consent, In other countries such as United State laws that require the use of age verification and/or age assurance methods are principally found in the context of legislation that seeks to prevent minors from accessing pornographic or other material deemed "harmful to minors" (**HTM**).[13] In addition, South Korea, have already adopted such systems. South Korea's "Shutdown Law" restricts online gaming for minors during night hours and requires parental consent for access to certain games.[14] This model provides a roadmap for Cambodia to follow. The responsibility for protecting minors should no longer fall solely on parents and must be shared by the platforms profiting from children's engagement.[15]

[5] Cambodia, "Law on consumer protection", 2009.
[6] Cambodia, "Civil Code", 2009.
[7] United Stated, Centre for information policy leadership, "age assurance and age verification law", 2024.
[8] Cambodia, "Civil Code", 2009, Article 17.
[9] Cambodia, "Civil Code", 2009, Article 17.
[10] Mondaq, "Through click-wraps are legal, can minor enter into click-wraps", 2023, https://www.mondaq.com/india/it-and-internet/1305896/though-click-wraps-are-legal-can-minors-enter-click-wraps.
[11] Ibid.
[12] UNICEF, "Cambodian child online protection guidelines for the digital technology insdustry", 2023, https://www.unicef.org/cambodia/media/7751/file/Cambodian%20Child%20Online%20Protection%20Guidelines.pdf.
[13] United State, "Age assurance and Age verification law in the US", 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_age_assurance_in_the_us_sept24.pdf.
[14] Korea, "Shutdown Law", Article 26.
[15] Ibid.

To enhance the protection of minors and ensure responsible online practices, Cambodia should enact a Prakas on Age Verification and Content Classification.[16] Age verification has long been a key method for safeguarding children from potential harm, as evidenced by traditional ID checks at shop checkouts. Implementing comprehensive age verification measures online can similarly prevent minors from engaging in activities that may expose them to risks, aligning with Civil Code Article 17, which states that minors should not be held liable for certain activities they undertake online.[17] This regulation would require digital platforms to adopt meaningful and reliable age-verification systems, not just simple "YES/NO" buttons to accurately determine users' ages. Such measures would enforce effective age gating, restrict access to inappropriate content, and ultimately protect minors from harm while ensuring compliance with legal standards.

# III. The Rising of Child Grooming in E-Sport Sector and the Urgent Need of Criminal Code Must Involve in the Digital Area

As E-sports platforms continue to add social features such as voice chat, private messaging, and user forums, they also create new vectors for child exploitation.[18] Online child grooming refers to the process where an adult uses the internet or digital communication platforms to form a relationship with a child, with the intent of sexually exploiting or abusing the child either online or later in-person.[19] Some of the children surveyed had engaged in potentially risky behavior in the previous year. Approximately 9% had met someone in person whom they had first got to know online. However, all children should be informed about the possible risks and taught how to engage responsibly and to take safety precautions, such as informing adults before meeting people whom they know online or only meeting in public places because some children in Cambodia were reported that they had shared naked images or videos of themselves online. While some children have been flirted with or groomed by adults.[20]

These activities count as sexual harassment, which the Criminal code of Cambodia fails to address that. As seen in section 2 regarding the other sexual assault, article 246 of Criminal Code, mentioned that "Touching, fondling or caressing the sexual organs or other part of a person without that person' s consent or coercing another person to perform such acts on the perpetrator himself or herself or a third person for the purpose of arousing the perpetrator or providing sexual pleasure to the perpetrator constitutes indecent assault".[21] This provision is rooted in an offline paradigm. It does not address the digital grooming process, where a predator may never meet the child in person but still cause psychological and emotional harm through sustained digital contact. This legislative gap means that a person who engages in sexualized conversations with a child over a game's chat function or manipulates a child into sharing explicit images may not be prosecutable under current law. As a result, law enforcement is left without the tools to intervene until after significant

[16] European Parliament, "Online Age verification methods for children", https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf.
[17] Ibid.
[18] IEEE Access, "Child safety and protection in the online gaming ecosystem", 2022, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9933399.
[19] UNICEF, "let's chat about online grooming", https://www.unicef.org/cambodia/lets-chat-about-online-grooming.
[20] UNICEF, "Disrupting Harm in Cambodia: Evidence on online child sexual exploitation and abuse." https://www.unicef.org/innocenti/media/4136/file/DH-Cambodia-Report-2022.pdf.
[21] Cambodia, "Criminal Code", article 246.

harm has occurred. Cambodian law has yet to catch up because the current law is defined to criminalize the physical procurement of minors for prostitution, trafficking, and the dissemination of pornographic content.

The United Kingdom's Sexual Offences Act 2003 makes it an offense for an adult to communicate with a child at least twice and arrange to meet with intent to abuse even if no physical contact has yet occurred.[22] This reflects a progressive understanding of the online threat, where psychological manipulation can be as harmful as physical abuse and requires legal intervention at the earliest stages. Introducing such provision would mark a major step forward in aligning Cambodia's criminal justice system with today's digital realities. It would provide law enforcement with the authority to act proactively and offer greater protection to children navigating online space. Moreover, it would create a legal obligation for online platforms particularly E-sports companies to monitor and moderate user interaction. Platforms that knowingly allow, ignore, or fail to address grooming behaviors could face civil or criminal penalties, encouraging safer design and more responsible moderation.

To address this, the Criminal Code must be amended to include a new provision specifically targeting online child grooming. Such a provision could define grooming as the act of using any form of digital communication including voice chat, direct messaging, or online forums to intentionally build a relationship with a minor with the intent of committing a sexual offense. Importantly, the law should not require physical contact or the exchange of explicit content to establish the offense. The mere act of initiating a manipulative relationship with intent should be criminalized.

# IV. Inadequate Legal Framework in Law on Consumer Protection for Digital Consumer Protection

One of the most pressing concerns is the lack of consumer protection. Currently, these digital transactions exist in legal grey areas. The main law that deals with consumer rights is the Law on Consumer Protection (**LCP**), promulgated by Royal Kram No. NS/RKM/1119/016 on November 2, 2019, provides general safeguards against fraud and deceptive business practices.[23] However, its current orientation towards traditional commerce limits its effectiveness in addressing the complexities inherent in the digital economy, particularly within the E-Sport Sector. Under the LCP, consumers are referring to any individual who acquires goods or services for personal, domestic, or household use and not for commercial purposes.[24] Consumers in this context include gamers (minors and adults), parents, viewers, players, and general users of the E-Sports platform. To ensure comprehensive consumer protection in the digital age, the following articles within the Law on Consumer Protection require substantive revision or expansion.

Article 3 of the LCP mentioned that "This law shall apply to any person who conducts a business, whether for a profit or for non-profit, including the sale of goods or services or real rights over immovable property, to consumers in the Kingdom of Cambodia unless otherwise provided by separate provisions."[25] However, in this context the terms "goods" and "service" are not clearly defined

[22] United Kingdom, "Criminal Act", 2003.
[23] Cambodia, "Law on Consumer protection", 2019.
[24] Cambodia, "Law on Consumer protection", 2019, Article 4.
[25] Cambodia, "Law on Consumer protection", 2019, Article 3.

to include digital products. The law focuses on physical items and in-person services, leaving out important digital elements like game "skin", "loot box", or "downloadable content". This creates a legal loophole, where consumers are left vulnerable in online transactions.

To close this gap, Article 3 should be updated to reflect the realities of today's digital economy and redefine the definition of the "digital goods" and "digital services." The definition could be expanded to "'Goods' shall mean any movable or immovable property, whether tangible or intangible, including digital goods such as video games, virtual items, in-game currency, and downloadable content. 'Services' shall include digital services such as online platform access, server use, digital streaming, and hosting of virtual events." By revising the law in this way, Cambodia can offer stronger consumer protection in the digital age, ensuring that E-sports participants and users are treated fairly, transparently, and safely just like consumers in any other marketplace.

# V. Minor Data Privacy Concern: The Urgent Need of Personal Data Protection Law

Currently, children spend a lot of time playing games online, but the gaming industry has received less scrutiny than social media or streaming platforms over privacy concerns. As gaming grows, the scale of user vulnerability increases as well. Many young people do not understand the data risks posed by online games.[26] Online games do not just collect basic information like names, ages, or locations. but also collect the amounts of behavioral data, including playtime patterns, social connections, in-game chat logs, and even emotional responses. For minors, this data is often collected without informed consent.[27] This is particularly alarming given recent findings. According to the report from UNICEF "Disrupting Harm in Cambodia: Evidence on online child sexual exploitation and abuse" revealed that 1 in 10 Cambodian children have already experienced online sexual abuse and exploitation, a risk amplified by unchecked data collection.[28] This makes it urgent for Cambodia to move forward with the long-awaited Draft Law on Personal Data Protection. The law must go beyond general protections and include strong, specific safeguards for minors. For example, companies should be required to obtain clear and verifiable consent from parents before collecting any personal information from users under 18. Children and their guardians must also be given the right to request deletion of their data at any time. Moreover, data collection should be limited to what is strictly necessary for the game to function, not used for hidden commercial purposes like ad targeting or behaviour prediction. Importantly, the responsibility for protecting children's data should fall squarely on the game developers and platform providers. These companies must be held accountable for ensuring that consent is properly obtained, and that data is used transparently and ethically.

By enacting this law, Cambodia would align itself with international standards such as the EU's General Data Protection Regulation and South Korea's child data laws. A requirement for explicit and verifiable parental consent for the collection, processing, and sharing of any personal data from individuals under the age of 18. The burden of proof for obtaining this consent must lie with the

[22] Elizabeth Denham, "Data protection trends in children's online gaming", September 10, 2022, https://iapp.org/news/a/data-protection-trends-in-childrens-online-gaming.
[23] Ibid.
[24] UNICEF, "Disrupting Harm in Cambodia: Evidence on online child sexual exploitation and abuse", https://www.unicef.org/innocenti/media/4136/file/DH-Cambodia-Report-2022.pdf.

data controller (i.e. the game company). Enacting this law is the single most important step Cambodia can take to protect children's privacy and safety online, creating a legal foundation for a "safer internet by design".

# VI. Conclusion

The rapid rise of E-sports in Cambodia signals a transformative shift in how entertainment, competition, and community are experienced in the digital age. However, this transformation has outpaced the country's legal and regulatory frameworks, leaving critical gaps in consumer protection particularly for children and who are the primary participants in this space. Across this brief, we have identified multiple pressing legal challenges, outdated definitions in the Law on Consumer Protection, the absence of age-verification and content control mechanisms, weak data privacy safeguards, the unchecked rise of online child grooming, and the use of manipulative game design strategies that fuel addiction. These issues are not isolated, they are deeply interconnected and symptomatic of a larger regulatory failure to recognize the unique dynamics and risks of digital gaming ecosystems. As a result, minors remain unprotected against harmful content and predators, consumers are misled by manipulative in-game mechanics, and vast amounts of personal data are collected with little accountability or transparency.

Cambodia must act on multiple fronts. First, it must modernize the Law on Consumer Protection by expanding key definitions and prohibiting deceptive and manipulative design practices that exploit psychological vulnerabilities. Second, the criminal code must be amended to criminalize online child grooming, ensuring that law enforcement has the tools to intervene before irreversible harm occurs. Third, the government shall urgently issue a Prakas on Age verification and content classification, ensuring that minors are not left exposed to inappropriate content or online exploitation due to poor platform design and liable to the consent. Finally, the draft law on Personal Data Protection must be passed with explicit safeguards for minors and binding obligations on gaming platforms regarding consent, data minimization and transparency. These legal reforms will not suppress innovation in the E-sports industry but foster an environment where innovation thrives alongside accountability, responsibility, and ethical standards. A forward-looking legal framework will not only protect consumers, especially vulnerable youth but also build public trust, guarantee minor's safety, and support the long-term sustainable development of Cambodia's digital economy. As Cambodia continues its digital journey, it must ensure that its laws evolve in step with technology. By doing so, the country can secure a future where the benefits of E-sports are maximized while the harms are minimized ensuring that the virtual worlds our youth inhabit are not only exciting and engaging, but also safe, inclusive, and respectful of their rights.

[29] EU, "General data protection regulation".


# Section 04

# Cybercrime Law

# From Bytes to Burden of Proof: Establishing Cambodia's Digital Evidence Framework


## ODOM Somnang

[Junior associate at Soksipha Sethalay & Associates]

Somnang Odom is a undergraduate law student pursuing a Bachelor of Law in the International Program of Legal Studies at the National University of Management. He has competed and advised in multiple international moot court competitions, including ICRC IHL, JHJ WTO, SKADDEN FDI, and IBA ICC. His current work focuses on litigation and arbitration cases, with particular interest in commercial dispute resolution and Cambodia's developing arbitration framework.


# I. Introduction

Cambodia faces significant challenges in handling digital evidence, primarily due to an underdeveloped legal framework.[1] The existing *Criminal Code (2009)* contains outdated.[2] provisions for computer-related offenses.[3] Furthermore, the *Criminal Procedure Code* (2007) lacks any comprehensive mechanisms to preserve volatile digital data.[4] The draft Law on Cybercrime, despite being in development since 2012, raises concerns about a broad interpretation and potential rights infringement.[5]

This legal ambiguity extends to the definition of *digital evidence* itself, as the Law on Electronic Commerce (2019), while touching on electronic evidence procedures[6] and admissibility,[7] fails to provide a comprehensive legal definition, leading to confusion and inconsistent practices.[8]

Furthermore, the volatile nature,[9] of digital evidence challenges its authenticity and admissibility, and without specific legal standards for authentication, it is challenging to demonstrate that the digital evidence presented in court is the same as the original data and has not been tampered with.[10]

[1] Open Development Cambodia, "1.2 Cybersecurity a key challenge," in Cybersercurity in Cambodia: Current Developments and Challenges Ahead (Phnom Penh: Open Development Cambodia Organization, 2023), 7.
[2] Open Development Cambodia, "Cybersecurity Legislation," 10.
[3] Open Development Cambodia, "Cybersecurity Legislation," in Cybersercurity in Cambodia: Current Developments and Challenges Ahead (Phnom Penh: Open Development Cambodia Organization, 2023), 10; Royal Government of the Kingdom of Cambodia, Criminal Code (Royal Government of the Kingdom of Cambodia, 2009), arts. 317–20, 427–32.
[4] Royal Government of the Kingdom of Cambodia. Criminal Procedure Code. Royal Government of the Kingdom of Cambodia, 2007.
[5] CyberCX, Cambodia and Australia's Department of Foreign Affairs and Trade, Cambodia Cyber Security Capability Assessment (CyberCX, 2022), 10.
[6] Royal Government of the Kingdom of Cambodia, Law on Electronic Commerce (Royal Government of the Kingdom of Cambodia, 2019), art. 42.
[7] Ibid., Art. 44-45.
[8] Stephen Mason, "Chapter 2: The Characteristics of Electronic Evidence," in Electronic Evidence: Disclosure, Discovery, and Admissibility (London: LexisNexis Butterworths, 2007), 23, ¶2.04.
[9] Association of Chief Police Officers, APCO Good Practice Guide for Digital Evidence (Police Central e-crime Unit, 2012), 36; Bill Nelson et al., "Processing Crime and Incident Scenes," in Guide to Computer Forensics and Investigations, 7th ed. (Boston: Course Technology Inc, 2024), 215.
[10] Stephen Mason, "Chapter 8: England & Wales," in Electronic Evidence: Disclosure, Discovery, and Admissibility (London: LexisNexis Butterworths, 2007), 190, ¶8.22–8.23.

Finally, the critical absence of explicit data preservation laws to prevent its deletion,[11] modification,[12] or overwriting,[13] hampers investigations, as there are no clear mandates for service providers to proactively preserve potentially relevant digital data, thereby impeding the prosecution of technology-related crimes, especially across jurisdiction boundaries.[14]

This analysis will strictly focus on the legal statutes, regulations, directives, and other relevant legal instruments governing digital evidence, examining (**II**) Statutory Authority and Law Enforcement Powers in Digital Investigation (**III**) Judicial Admissibility Standards for Digital Evidence (**IV**) Professional Competency Standards for Digital Forensic Practitioners and Expert Testimony (**V**) International Cooperation and Transnational Evidence Acquisition.

# II. Statutory Authority and Law Enforcement Powers in Digital Investigation

A key distinction lies in who primarily wields the power and under what oversight. Cambodia allows digital access powers mainly through court approval, where investigating judges can order the interception of phone calls, emails, and faxes under CPC Article 172. At the same time, the *E-Commerce Law* forbids encrypting data that could be used as evidence in criminal cases, suggesting authorities can demand such data be unlocked. The Criminal Code criminalizes illegal computer access, providing legal grounds for digital investigations. Singapore's *Criminal Procedure Code* (2010) Section 39 grants significant statutory powers directly to the police and investigators, with the Public Prosecutor under *CPC* Section 40 authorization required for decryption orders.[15] This contrasts with Cambodia, where the primary specific power identified for digital intrusion (interception) requires an order from an investigating judge.[16] Regarding territorial reach, Singapore's T*elecommunications Act* (1999) Section 58 explicitly provides for police remote access to computers outside its borders under certain conditions,[17] representing a direct assertion of extra-territorial investigative power. Cambodia appears reliant on formal Mutual Legal Assistance procedures for cross-border evidence gathering.[18] Singapore's framework offers efficient statutory powers with prosecutorial oversight and explicit extraterritorial capabilities that address digital evidence's urgent, cross-border nature.

Furthermore, the EU's harmonized approach via the *E-Evidence Package* centers on judicial authorities issuing cross-border orders under the *European Production Order* (**EPOC-RC**), directed specifically at service providers, reflecting a system structured around inter-state judicial cooperation.[19] The authority to compel decryption or the disclosure of access credentials is most explicit in Singapore's framework.[20] The EU framework, including the *E-Evidence Regulation* (**EU**) 2023/1543 and the Buda-

[11] Nelson et al., "Common Extraction Methods," 532; Mason, "United States of America," 490, ¶16.05.
[12] Anita Gehlot et al., "7.6 Role of Digital Forensics in Cybercrime Investigation for IoT," in Digital Forensics and Internet of Things: Impact and Challenges (Beverly, MA: Scrivener Publishing, 2022), 100.
[13] Gehlot et al., "IoT Forensics," 259, ¶15.12; Mason, "United States of America," 490, ¶16.05.
[14] Nelson et al., "Jurisdiction Issue," 479.
[15] Singapore, Criminal Procedure Code 2010, No. 15 of 2010, Singapore Statutes Online, accessed May 17, 2025, https://sso.agc.gov.sg/Act/CPC2010.
[16] United Nations Office on Drugs and Crime (UNODC), "Electronic Evidence Fiche: CAMBODIA," SHERLOC, accessed April 17, 2025, https://sherloc.unodc.org/cld/uploads/pdf/EI%20Evidence%20Hub/Electronic_Evidence_Fiche_as_of_18_January_CAMBODIA.pdf.
[17] Christopher SJ Ong, "Legislative Framework for Fighting Cybercrime" (presentation, 2nd ACCPCJ, Thailand Institute of Justice, Bangkok, Thailand, n.d.), accessed April 17, 2025, https://www.tijthailand.org/public/files/highlight/2nd%20ACCPCJ/presentation/T5_Mr.%20Ong.pdf.
[18] UNODC, "Electronic Evidence Fiche: CAMBODIA."
[19] Baker McKenzie, "New EU regulation on digital evidence opens up risk of data misuse," Connect On Tech, February 2024, accessed April 17, 2025, https://connectontech.bakermckenzie.com/new-eu-regulation-on-digital-evidence-opens-up-risk-of-data-misuse/.
[20] Singapore, Criminal Procedure Code 2010.

pest Convention, primarily targets access to existing data held by service providers.[21] While the *Budapest Convention and Directive* 2013/40/EU include powers like search, seizure, and harmonizing offences that might encounter encryption, the EU instruments do not create a harmonized obligation for individuals to decrypt data, leaving this largely to national laws, and acknowledging encryption as a challenge.[22]

While inherently cross-border, the EU's E-Evidence mechanism operates through formal orders transmitted to service providers via their designated representatives or establishments within the enforcing Member State, thereby respecting territoriality through a structured legal process.[23] The *EU's E-Evidence* framework provides structured judicial oversight for cross-border digital evidence while respecting territoriality and enabling efficient inter-state cooperation.

To address urgent investigative needs while comprehensive cybercrime legislation is finalized, Cambodia should issue a supplementary *Prakas* (**Proclamation**) under the existing Law on E-Commerce. This interim regulation should establish three critical provisions: first, expanded definitions of "digital evidence" and "electronic data" to encompass cloud storage, social media communications, and encrypted materials; second, mandatory data preservation requirements compelling internet and cloud service providers to maintain potentially relevant evidence for specified periods upon official request; and third, standardized procedures for law enforcement to initiate preservation requests with appropriate judicial oversight.

# III. Judicial Admissibility Standards for Digital Evidence

Cambodia follows a broad evidence admissibility rule under CPC Article 321, allowing all evidence types in criminal proceedings unless specifically excluded by law.[24] Moreover, the assessment of evidence falls to the court, which considers its value based on the judge's "intimate conviction".[25] Judgments must be based solely on evidence in the case file or presented during the hearing.[26]

E-Commerce Law requires electronic evidence (**Annex Definition 17**) to meet authenticity standards. However, the lack of detailed statutory procedures for digital evidence handling may create practical challenges in consistently demonstrating integrity and authenticity, potentially affecting the weight courts assign to such evidence despite its technical admissibility.[27]

Singapore and Cambodia present contrasting approaches to specificity. Singapore's Section 116A of the *Evidence Act* (2021) transitioned from highly detailed rules for "computer output" to a general relevance-based standard for all electronic evidence, reflecting adaptation to adaptation.[28] The EU stands apart, although the *Treaty on the Functioning of the European Union* (**TFEU**) Article 82(2)(a) grants the EU competence to adopt minimum rules concerning the mutual admissibility of evidence

[21] Baker McKenzie, "New EU regulation."
[22] European Commission, High-Level Group on Access to Data for Effective Law Enforcement, "Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement," November 2022, accessed April 17, 2025, https://home-affairs.ec.europa.eu/system/files/2022-11/Recommendations%20of%20the%20HLG%20on%20Access%20to%20Data%20for%20Effective%20Law%20Enforcement_en.pdf.
[23] Reed Smith, "The e-Evidence Regulation: A New EU Legal Framework for cross-border access to electronic evidence," Viewpoints (blog), August 27, 2024, accessed April 17, 2025, https://viewpoints.reedsmith.com/post/102jfw4/the-e-evidence-regulation-a-new-eu-legal-framework-for-cross-border-access-to-el.
[24] UNODC, "Electronic Evidence Fiche: CAMBODIA."
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ong, "Legislative Framework."
[29] eucrim – The European Criminal Law Associations' Forum, "Mutual Admissibility of Evidence and Electronic Evidence in the EU," eucrim, October 19, 2023, accessed April 17, 2025, https://eucrim.eu/articles/mutual-admissibility-of-evidence-and-electronic-evidence-in-the-eu/.

between Member States, specifically to facilitate mutual recognition of judgments and judicial cooperation, the absence of harmonized admissibility rules at the Union level; admissibility remains fragmented and governed by the diverse national laws of its Member States, which creates potential friction despite harmonized cross-border evidence gathering mechanisms.

Concerns about authentication and integrity are universal but addressed through different legal techniques. Singapore utilizes a statutory presumption linked to certified processes under its *Evidence Act.*[30] Cambodia relies on a general requirement of authenticity mandated by its E-Commerce Law, coupled with the judge's assessment.[31] In the EU context, while national rules dictate formal admissibility, there is a discernible trend towards viewing compliance with technical standards and best practices (like those from ENFSI or the Council of Europe's EEG) as crucial indicators of reliability and integrity, influencing judicial assessment even if not always a strict legal requirement for admissibility.[32]

The handling of evidence obtained via international cooperation also differs. Cambodia's law explicitly mandates the admission of evidence received through MLA.[33] In the EU, evidence obtained using the new E-Evidence Regulation's *EPOC/EPOC-PR* mechanism must still satisfy the national admissibility requirements of the prosecuting Member State.[34] This highlights a potential gap between the facilitated *acquisition* of cross-border evidence and its ultimate usability in court. Singapore's admissibility rules under the Evidence Act apply generally to evidence regardless of its origin, including that obtained via its extra-territorial powers or MLA.

Cambodia should enact specific amendments to the *Criminal Procedure Code* to establish standardized admissibility criteria for digital evidence. The amendments should codify authentication requirements, including chain of custody protocols, hash verification, and metadata integrity standards. Additionally, they should create rebuttable presumptions of authenticity for evidence meeting *ISO 27037* or equivalent technical standards and establish differential admissibility thresholds, maintaining mandatory admission for MLA-obtained evidence while requiring enhanced authentication for evidence gathered through bilateral agreements or emerging cross-border mechanisms.

# IV. Professional Competency Standards for Digital Forensic Practitioners and Expert Testimony

A clear divergence exists in the formalization of standards for digital forensic practitioners. Currently, there are no laws, references, regulations, or mandatory certifications in Cambodia specifically for digital forensics professionals or expert witnesses in the Cambodian legal system.[35]

The EU context, heavily influenced by the European Network of Forensic Science Institutes (**ENFSI**),

[30] KPMG International, "Evidence Act Certification," December 2017, accessed April 17, 2025, https://assets.kpmg.com/content/dam/kpmg/sg/pdf/2017/12/Evidence-Act-certification-brochure.pdf.
[31] UNODC, "Electronic Evidence Fiche: CAMBODIA."
[32] European Law Institute (ELI), ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings, 2020, accessed April 17, 2025, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf.
[33] UNODC, "Electronic Evidence Fiche: CAMBODIA."
[34] eucrim, "Mutual Admissibility."
[35] Interpol, "The Use of Digital Evidence in Prosecutions in Asia: Executive Summary," 2022, accessed April 17, 2025, https://www.interpol.int/content/download/17171/file/The%20Use%20of%20Digital%20Evidence%20in%20Prosecutions%20in%20Asia....pdf.

emphasizes structured professional standards, documented best practice manuals (**BPMs**), and frameworks for competence assessment, even without legally mandated EU-wide individual certification.[36] Singapore, in contrast, relies on the general provisions for expert evidence within its Evidence Act, with courts assessing competence and impartiality on a case-by-case basis using criteria developed through jurisprudence.[37] Cambodia currently appears to lack specific legal requirements or widely adopted professional standards for digital forensic experts, although training based on international norms is available.[38]

The understanding of 'competence' itself reflects these differing approaches. ENFSI provides a broad definition encompassing knowledge, skills, behavior, and attitude.[39] Singaporean courts focus on knowledge, familiarity, relevant practical experience, and critically, the expert's impartiality and duty to the court.[40] While general qualifications recognized in the international field, such as specific certifications like *Certified Forensic Computer Examiner (***CFCE***) or Certified Information Systems Security Professional* CISSP[41] likely hold value in all jurisdictions, their formal legal weight and necessity vary. The absence of specific Cambodian rules makes formal assessment criteria there unclear beyond general witness credibility evaluations.

Laboratory accreditation (e.g., to ISO 17025) and adherence to established best practice guidelines like ENFSI BPMs or the UK's ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence,[42] are more established as indicators of reliability within the EU framework, and likely influence practice in Singapore as well. These provide a mechanism for demonstrating procedural rigor and quality assurance, which can be crucial in court, especially where individual practitioner certification is not mandated by law. Singapore's system for certifying processes under the Evidence Act,[43] is distinct from accrediting the competence of individual examiners or laboratories performing forensic analysis.

Cambodia should enact specific provisions within the Criminal Procedure Code defining competency requirements for digital forensic expert witnesses. The legislation should establish mandatory minimum qualifications, including recognized international certifications such as CFCE, CISSP, or equivalent credentials, documented training in digital forensics methodologies, and practical experience requirements. Furthermore, it should implement laboratory accreditation standards requiring ISO 17025 compliance or equivalent quality management systems for forensic facilities, alongside procedural obligations for expert witnesses, including adherence to established best practice guidelines such as ENFSI BPMs, maintenance of chain of custody documentation, and disclosure of methodology and limitations.

These standards should be enforced through a judicial certification process administered by the Ministry of Justice and the Ministry of Interior, creating a registry of qualified digital forensic experts. Unlike Singapore's case-by-case judicial assessment or the EU's voluntary professional frameworks,

[36] European Network of Forensic Science Institutes (ENFSI), "Best Practice Manuals and Forensic Guidelines," accessed April 17, 2025, https://enfsi.eu/about-enfsi/structure/working-groups/documents-page/documents/best-practice-manuals/.
[37] David LLEWELYN, "The use of experts in legal proceedings in Singapore involving intellectual property rights," Singapore Management University School of Law Research Collection, 2016, accessed April 17, 2025, https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=5205&context=sol_research.
[38] Interpol, "Use of Digital Evidence in Asia."
[39] European Network of Forensic Science Institutes (ENFSI), "Guidance on the Assessment of Competence for Forensic Practitioners," QCC-CAP-006-001, November 2017, accessed April 17, 2025, https://enfsi.eu/wp-content/uploads/2017/11/QCC-CAP-006-001.pdf.
[40] Agnes Lo, "Evidence Admissibility of Expert Opinions," Juris Illuminae, Singapore Law Review, 2019, accessed April 17, 2025, https://www.singaporelawreview.com/juris-illuminae-entries/tag/Agnes+Lo.
[41] Purpose Legal, "The Role of Digital Forensics Expert Witnesses," JDSupra, May 2, 2022, accessed April 17, 2025, https://www.jdsupra.com/legalnews/the-role-of-digital-forensics-expert-4087503/.
[42] IntaForensics, "Computer, Mobile Phone and Cell Site Analyst," accessed April 17, 2025, https://www.intaforensics.com/df-expert-witness/.
[43] KPMG, "Evidence Act Certification."

Cambodia's codified approach would provide legal certainty while ensuring international compatibility. The framework should include provisions for reciprocal recognition of foreign laboratory accreditations and expert qualifications, facilitating cross-border cooperation while maintaining domestic quality control.

# V. International Cooperation and Transnational Evidence Acquisition

Cambodia appears to be the most constrained in its options for international cooperation. Its explicit prohibition on direct requests to providers,[44] and its non-participation in the Budapest Convention,[45] leave it heavily reliant on the formal, potentially slower, state-to-state MLA process governed by its 2020 law and the ASEAN MLAT.[46] While its MLA law allows cooperation based on reciprocity even without a treaty,[47] the inherent delays in formal MLA can be particularly detrimental when dealing with volatile digital evidence.[48]

The most striking difference lies in the EU's development of a bespoke, streamlined intra-EU system, the *E-Evidence Package* for accessing specific types of cross-border digital evidence held by service providers.[49] This moves beyond the traditional state-to-state MLA model relied upon primarily by Singapore and Cambodia.[50] While the E-Evidence Package aims for speed and efficiency within the EU, its effectiveness depends on successful implementation and interaction with national laws.

Singapore occupies a unique position due to its combination of traditional MLA via its *Mutual Assistance in Criminal Matters Act,*[51] active participation in the premier international instrument, the *Budapest Convention,*[52] and its domestic law allowing direct extra-territorial access under specific circumstances, *Criminal Procedure Code* Section 39.[53] This provides Singaporean authorities with a more diverse toolkit for cross-border access compared to Cambodia, and potentially faster or more unilateral options in some cases than available even through the EU's formal mechanisms. However, the *E-Evidence Package* specifically targets speed.

Cambodia should prioritize accession to the *Budapest Convention on Cybercrime* as a foundational step to address its current cross-border digital evidence cooperation constraints. Accession would provide three critical benefits: first, access to the Convention's 24/7 network for urgent preservation requests, directly addressing the volatility of digital evidence that makes traditional MLA procedures inadequate; second, a comprehensive legal framework to guide domestic cybercrime legislation development, ensuring international compatibility and reducing the risk of legal gaps that currently limit cooperation options; and third, structured capacity-building programs and technical assistance to strengthen judicial and law enforcement capabilities.

[44] UNODC, "Electronic Evidence Fiche: CAMBODIA."
[45] Council of Europe, "Cambodia," Octopus Cybercrime Community, accessed April 17, 2025, https://www.coe.int/en/web/octopus/-/cambodia.
[46] UNODC, "Electronic Evidence Fiche: CAMBODIA."
[47] Kingdom of Cambodia, Ministry of Justice, "Basis and Kinds of Assistance in MLA Law," 2022, accessed April 17, 2025, https://moj.gov.kh/files/user-folder/2022/MLA/01-Basis%20and%20Kinds%20of%20Assistance%20in%20MLA%20Law.pdf.
[48] Government of Singapore, "Singapore Contribution on General Provisions, Criminalisation, and Procedural Measures and Law Enforcement," submission to the Ad Hoc Committee on Cybercrime, Second Session, United Nations Office on Drugs and Crime, May 2022, accessed April 17, 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Singapore_statement.pdf.
[49] Baker McKenzie, "New EU regulation."
[50] Cambodia, Ministry of Justice, "Basis in MLA Law."
[51] Attorney-General's Chambers Singapore, "Mutual Legal Assistance," accessed April 17, 2025, https://www.agc.gov.sg/our-roles/international-law-advisor/mutual-Legal-assistance.
[52] Council of Europe, Convention on Cybercrime, CETS No. 185, opened for signature November 23, 2001, entered into force July 1, 2004.
[53] Ong, "Legislative Framework."

Beyond these immediate advantages, Convention membership would position Cambodia to engage with emerging cross-border mechanisms, including potential future ASEAN digital evidence cooperation frameworks. The Convention's flexible approach to implementation would allow Cambodia to maintain its current MLA-centric approach while gaining additional tools for urgent cases. Given Cambodia's current prohibition on direct provider requests and exclusion from faster bilateral mechanisms available to Singapore, the Budapest Convention represents the most viable path to expand its international cooperation toolkit without compromising sovereignty or requiring complex bilateral negotiations.

# VI. Conclusion

Cambodia's digital evidence framework reveals a complex web of legal gaps that fundamentally undermines the country's capacity to prosecute technology-related crimes effectively. The analysis demonstrates that while neighboring Singapore has developed sophisticated statutory powers and the EU has established harmonized cross-border mechanisms, Cambodia remains constrained by outdated legislation, absent professional standards, and limited international cooperation tools. The proposed solutions, including interim Prakas regulations, Criminal Procedure Code amendments establishing authentication standards, mandatory expert competency requirements, and Budapest Convention accession, represent a comprehensive roadmap for legal reform. However, the urgency of these reforms cannot be overstated, as Cambodia's current legal ambiguity not only hampers domestic investigations but also isolates the country from international cooperation networks essential for combating transnational cybercrime. Without immediate legislative action, Cambodia risks becoming a haven for digital criminal activity while simultaneously being unable to protect its own citizens from cyber threats that increasingly transcend national boundaries.

# Delimiting freedom of expression in Deepfakes: Tackling Malignant Deepfake Personality Rights Violation in Identity Theft and Non-Consensual Intimate Imagery Deepfakes

**RATTANA Sokunthyda**

[Junior law student at the National University of Management]

She is an awardee of the 2025-2026 Global UGRAD Exchange Program. She has participated in the 16th Nelson Mandela World Human Rights Moot where her team's memorial ranked 4th out of the 92 participating teams, and she was also a National Champion of the 2025 Red Cross International Humanitarian Law Moot. Previously, she was also a Political Intern at the US Embassy in Phnom Penh.

## I. Introduction

Among recent artificial intelligence (**AI**) innovations, 'deepfake' is most prone to misuse due to its accessibility and capabilities in blurring our perceptions of reality. Deepfake (**Deep fake**), is commonly defined as, "synthetic media, including images, video, and audio generated by AI technology that portrays something that does not exist in reality or events that have never occurred".[1] This technology frequently creates global headlines with frauds,[2] disinformation campaigns, intellectual property (**IP**) infringements, and most alarmingly non-consensual intimate imagery (**NCII**), accounting for an estimated 98% of deepfakes online.[3] These are essentially violations of 'personality rights'.

Personality rights (*Right to Publicity*), originated from the right to privacy, refer to the rights to protect, control, and profit from one's image, name, or likeness.[4] It consists of two facets: (1) the right for one's image to be protected from commercial exploitation (*right of publicity*); and (2) the right to be left alone, which concerns non-economic damages (*right to privacy*).[5]

Conventionally, generating deepfakes is a protected

[1] Payne, L. "deepfake." Encyclopedia Britannica, (May 7, 2025). https://www.britannica.com/technology/deepfake.
[2] Blake Hall, "How AI-Driven Fraud Challenges the Global Economy – and Ways to Combat It," World Economic Forum, (June 4, 2025), https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/.
[3] "The new face of digital abuse: Children's experiences of nude deepfakes", Internet matters, (October 2024). p.14. https://www.internetmatters.org/wp-content/uploads/2024/11/Childrens-experiences-of-nude-depfakes-research.pdf.
[4] Luthra S. Krishan and Vasundhara Bakhru, "Publicity Rights and the Right to Privacy in India," National Law School of India Review 31, no. 1 (2019): p. 125.
[5] Ibid., 125-26.

form of freedom of expression (**FOE**), like many other content creations. However, this protection is not absolute as malignant deepfakes require judicial interventions and limitations when they infringe on others' rights. With a trending increase in online access and low digital literacy (only 5% of the population possesses intermediate digital literacy),[6] Cambodia is particularly vulnerable to malignant deepfakes harms, notably in identity theft through online impersonation[7] and NCII.[8]

This vulnerability is exacerbated by Cambodia's lack of a comprehensive framework, hindering victims from acquiring timely injunctive relief and other remedies. However, regulating deepfakes brings along the FOE delimitation conundrum, as some deepfakes are benign— for instance, celebrity parodies, or deepfake videos educating about deepfake risks, are actually lawful expressions.[9] Moreover, a blanket ban would critically undermine the FOE and, consequently, innovation and democracy.

This brief seeks to identify a comprehensive and holistic solution for malignant deepfakes in identity theft and NCII. Evaluations will be made on Cambodia's legal framework readiness, by examining its statutory protections on FOE and personality rights pursuant to the International Covenant on Civil and Political Rights (**ICCPR**); and piecemeal legislations including, Law on suppression of human trafficking and sexual exploitation (**LSHTSE**), Inter-Ministerial Prakas No. 170, Criminal and Civil Codes. Additionally, comparative insights will be made on the United States (US) and Singapore's jurisdictions to identify evolving international solutions. The California Penal Code (**CPC**) Section 528.5 and the Fair Use doctrine, together, offer a holistic framework by penalizing traditionally overlooked non-economic harms from such personality rights violations, while safeguarding FOE from over-regulation. Meanwhile, Singapore's Penal Code and Protection from Harassment Act (**POHA**), also similarly able to address those harms within its conservative political framework. These comparative insights from jurisdictions with varying free speech protection offer an adaptable and holistic solution for Cambodia's legal reform.

# II. Cambodian Legal Framework Limited Readiness for Regulating Malignant Deepfakes

## 1. Cambodia Constitution: Bridging the International Standards

The Constitution's Article 31 explicitly recognises the kingdom's obligation under the international human rights conventions. Both Article 31 and 41 echo the standards held by Article 19 of the ICCPR, where citizens' enjoyment of personal rights and freedom is limited from adversely affecting that of others.[10] Additionally, personality rights are also guaranteed within the 1993 Constitution Article 32 (right to security), and Article 38 (the law shall protect the life, honor, and dignity of citizens).[11] These provisions are a great foundation in guiding the government's regulation of deepfakes, which usually have inevitable implications on these fundamental rights.

[6] "Cambodia launches its first competency framework on Digital, Media and Information Literacy to empower citizens in today's digital society", UNESCO, (July 4, 2024). https://www.unesco.org/en/articles/cambodia-launches-its-first-competency-framework-digital-media-and-information-literacy-empower.
[7] Hang Punreay, "Ministry of Post warns about AI-driven online scam", Khmer Times, (Feb 5, 2025), https://www.khmertimeskh.com/501634560/ministry-of-post-warns-about-ai-driven-online-scam/.
[8] "Taing Rinith, "Rise in non-consensual porn production involving Cambodian women," Khmer Times, (May 15, 2025), https://www.khmertimeskh.com/501677993/rise-in-non-consensual-porn-production-involving-cambodian-women.
[9] Alex Barber, "Freedom of expression meets deepfakes", Synthese 202, 40, (July 20, 2023), p.5. https://doi.org/10.1007/s11229-023-04266-4.
[10] The 1993 Constitution of the Kingdom of Cambodia, (September 21, 1993), Art.31, 41.
[11] Ibid., Art.32, 38.

## 2. Cambodia's Criminal Laws and Malignant Deepfakes

Amongst the many malignant deepfake threats, the two most urgent ones for Cambodia are identity theft and NCII, which are both covered within Cambodia's criminal laws to a certain extent. However, these piecemeal legislations often hinder victims seeking effective recourse and redress, and subsequently hinder effective suppression of such harms. In this section, relevant identity theft and NCII deepfakes provisions will be evaluated for their recourse and redress efficacy.

### A. Identity Theft via Online Impersonation: Addressing Non-Economic Harms

Identity theft (or identity fraud) is the unauthorized use of an individual's personally identifying information by someone else without that individual's permission or knowledge,[12] it includes online impersonations on social media, or any digital impersonations to commit crimes or enjoy privileges.[13] While resembling a 'Fraud' offense within the Criminal Code, criminalizing false identity usage, abusing a genuine identity of a third-party for certain illegal activities.[14] However, the stealing of personal information (initiating another identity theft) is not covered. And while Article 540 criminalizes the use of another person's 'name' which causes prosecution against the name-owner,[15] this is insufficient for online impersonation's versatile means. Even without active crimes, the impending legal troubles alone can bring victims insurmountable emotional distress. For instance, a social media account with the victim's photo impersonating him/her, sending intimate images privately, or rude comments online— besides legal disputes, it can cause interpersonal relations breakdown, psychological distress, or real-life personal safety risks.[16] Further, there is a lack of a swift recourse method to prevent further damages to the victims and others, such as a victim's certificate, before court proceedings.[17] With deepfakes, online impersonations become more convincing and fast-paced, posing a myriad of legal risks for ordinary citizens.

### B. NCII Deepfakes: A Lack of Injunctive Relief

For NCII deepfake (*i.e. pornographic or sexually explicit deepfake*), while the Code's Article 305 'Defamation', may appear to be applicable as it criminalizes false claims intended to publicly damage reputations via verbal, publication, or any public audio-visual communication. However, the real harm is not only in the defamatory intention; otherwise, there would be no offense, when there is a disclaimer or watermark disclosing the deepfake, dissociating the person presented from the forged content.

Although it is associated with many violations, the real issue lies in the obscenity of this personality rights violation, where even without defamatory intention, there exists emotional distress once victims discover the deepfakes.[18] There is an apparent intention to violate the victims' rights, neglecting their autonomy over their image. Hence, legislation targeting such aspects is a more suitable approach, which is within the LSHTSE.

According to J.D. Harris, the term "depict" in statutes enables its applicability to personal deepfakes,

[12] Radin, T.J. (2025, May 7). "identity theft". Encyclopedia Britannica. https://www.britannica.com/topic/identity-theft.
[13] Office of the Australian Information Commissioner (OAIC), "Identity fraud", (accessed May 13, 2025), https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/identity-fraud.
[14] Criminal Code of the Kingdom of Cambodia-English Translation, (2009), Art.377. https://www.licadho-cambodia.org/safety-and-justice/laws/criminal_code-2009-khmer+english-sithi.pdf.
[15] Criminal Code of the Kingdom of Cambodia-English Translation, (2009), Art.540.
[16] Colleen M. Koch, "To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation", University of Colorado Law Review 88, no. 1 (2017): p.244-46.
[17] Australian Government Attorney-General's Department, Application for a Commonwealth Victims' Certificate, (17 January 2024), https://www.ag.gov.au/national-security/publications/application-commonwealth-victims-certificate.
[18] Alex Barber, "Freedom of expression meets deepfakes". (July 20, 2023), p.5.

as it allows for interpretations to encompass virtual, realistic portrayals of individuals.[19] The Merriam Webster Dictionary defines "depict" as "to represent or as if by a picture", which includes drawing, photograph, movie, or even with words.[20] Correspondingly, LSHTSE provisions respectively defined "Pornography" and "Child Pornography" with the terms "visible material" and "depicting". These terms properly encompass any material formats visible to human vision. Both provisions' threshold for explicitness is relatively minimal— for Article 38, the depiction of a private part suffices, whereas the depiction of a minor's nudity suffices in Article 40.[21] Additionally, it punishes the entire cycle of such contents, including production, distribution, sale, lease, displaying the content in public place.[22] The low threshold and wide protection of this law (whether consensual or non-consensual) work in favor of prosecuting the viral nature of NCII deepfakes. Although it raises FOE concerns, this is in line with this nation's criticality towards upholding women's dignity, enshrined within its own Constitution.[23]

Nonetheless, a loophole remains as victims lack swift injunctive relief for content removals before court decisions. As seen in Taylor Swift's pornographic deepfake incident on X, time is of the essence for deepfake victims.[24] Furthermore, challenges exist in tracking down offenders, as many operate abroad and can skillfully conceal their tracks.

### 3. Tort Remedies in Cambodian Legal Framework

Cambodian Civil Code provisions explicitly recognizes the protection of the right to privacy,[25] additionally stipulating the injured party's rights to claim damages, restitution or injunctive relief, for intentional or neglectful infringement on their rights or benefits.[26] Injunctive relief is deemed most viable in preventing further damages from the identity theft, or NCII deepfakes, for victims, by requiring internet service providers, or platforms, to suspend the illegal accounts and/or take down the contents before court proceedings.[27] Harms to honor or reputation may also be remedied with both damages and a published apology.[28]

Favorably, the Inter-Ministerial Prakas No. 170 offers law enforcement a framework for managing news or content publication using Cambodia's internet. Clause 7 mandates the Ministry of Post and Telecommunications to collaborate with international institutions in blocking or removing websites, or social media pages engaged in activities deemed dangerous to public interests,[29] and publications of NCII deepfakes fall within the scope of national culture and tradition.[30] However, concerns remain with the lack of a mandated timeframe for illegal content removal and the arbitrary removal

## III. Comparative Analysis of Deepfakes Regulations in the US & Singapore

[19] Douglas Harris, "Deepfakes: False Pornography is Here and the Law Cannot Protect You," Duke Law & Technology Review 1, No. 17 (2019): p.103.
[20] Merriam-Webster.com Dictionary, s.v. "depict," (accessed April 17, 2025), https://www.merriam-webster.com/dictionary/depict.
[21] Kingdom of Cambodia, Law on Suppression of Human Trafficking and Sexual Exploitation (LSHTSE), (December 20, 2007), Art.38 & 40.
[22] LSHTSE, (December 20, 2007), Art.39 & 41.
[23] Constitution of the Kingdom of Cambodia, (September 21, 1993), Art.46(1).
[24] Emine Saner, "Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in her box," The Guardian, (January 31, 2024), https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box.
[25] Civil Code of the Kingdom of Cambodia, English translation by JICA (2007), Art.10-11.
[26] Civil Code of the Kingdom of Cambodia, (2007), Art.742-743.[5] Ibid., 125-26.
[27] Laura Dobberstein, "India requires platforms to remove deepfakes in 36 hours", The Register, (November 9, 2023), shttps://www.theregister.com/2023/11/09/india_deepfake_takedown/.
[28] Civil Code of the Kingdom of Cambodia, (2007), Art.757.
[29] Kingdom of Cambodia, Inter-Ministerial Prakas No. 170 on Publication Controls of Website and Social Media Processing via Internet in the Kingdom of Cambodia, (May 28, 2018), Clauses 1–3.
[30] "Hun Sen Vows to Crackdown on Indecent Online Adverts", Cambodianess, (Feb 17, 2020), https://www.cambodianess.com/article/hun-sen-vows-to-crackdown-on-indecent-online-adverts.

## 1. United States Balancing Regulation and Freedom of Expression: California Penal Code, and Fair Use Doctrine

Traditionally, the US's First Amendment offers FOE broad protections,[31] propelling innovations. However, some innovations have harmful uses, like malignant deepfakes, requiring regulation. Indiscriminate bans are unfeasible since benign deepfakes are lawful expressions. The US's targeted legislations with necessary exceptions, reflected in the CPC,[32] and the Fair Use doctrine,[33] establish a holistic framework suited for the complexities in countering the non-economic harms from deepfakes personality rights violations while balancing FOE.

### A. Tackling Online Impersonation on Social Media Platforms

The "Federal Identity and Assumption Deterrence Act of 1998" criminalizes the intentional unauthorized transfer or use of another person's identity for criminal intents, and with the Federal Trade Commission (FTC) designated in overseeing the 'Identity Theft' registry, assisting victims and forwarding complaints to appropriate agencies.[34] However, this act mostly focuses on the economic harms, making non-economic harm cases more likely to be dismissed.

A better developed legislation is found within the CPC Section 528.5, which penalizes any person who knowingly or non-consensually credibly impersonates another actual person through or on an internet website or any other electronic means for purposes of harming, intimidating, threatening, or defrauding.[35] This statute diverges from the traditional approach, which limits this to tort liability. Arriving at the right period where young people readily share too much information and trust others online, leading to real-life dangerous consequences.[36] As seen in the attempted killing of a San Diego woman,[37] and Megan Meier's case.[38] With deepfake technologies, online impersonations is conveniently on the rise.[39]

### B. Balancing FOE in Deepfakes with Fair Use Doctrine

Although lawful, benign deepfakes' non-consensual use of online content would raise IP rights concerns, without the 'Fair Use' doctrine of the Copyright Act.[40] Formulated to prevent Copyrights rigid application, stifling the FOE it was meant to foster;[41] this doctrine eliminates the barrier acquiring copyrights holders' licensed consent by offering exceptions to transformative use of works for purposes such as, criticism, comment, news, teaching, research, parody, satire and even artistic appropriation.[42] Fair use has four cumulative tests: [43]

- the purpose and character of the use (commercial or nonprofit educational purposes);
- the nature of the copyrighted work;
- the amount and substantiality of the portion used compared to the copyrighted work as a whole;

[31] "First Amendment", Legal Information Institute, Cornell Law School. https://www.law.cornell.edu/wex/first_amendment.
[32] California Penal Code, §528.5 (2011).
[33] U.S. Congress. United States Code: Copyrights, 17 U.S.C. (1978), §107.
[34] Identity Theft and Assumption Deterrence Act, 105th Cong. §512 (1997–1998), https://www.congress.gov/bill/105th-congress/senate-bill/512.
[35] California Penal Code, §528.5, (2011).
[36] Reznik Maksim, "Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation," Touro Law Review: Vol. 29: No. 2, (United States, 2013) Article 12. p.472-76. https://digitalcommons.tourolaw.edu/lawreview/vol29/iss2/12.
[37] Monica Garske, "Man Accused of Stalking Woman in Catfish Dating Hoax", NBC 7 SAN DIEGO (Aug. 29, 2013), https://www.nbcsandiego.com/news/local/brian-curtis-hile-insterstate-stalking-catfish-online-dating-scam/1958584/.
[38] "Parents: Cyber Bullying Led to Teen's Suicide", ABC News, (February 19, 2009), https://abcnews.go.com/GMA/story?id=3882520&page=1
[39] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), "Criminal Exploitation of Generative Artificial Intelligence," (December 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203.
[40] United States Code: Copyrights, 17 U.S.C. (1978), §107.
[42] "Copyright and Fair Use: A Guide for the Harvard Community", Office of the General Counsel, Harvard University, (January 10, 2024), https://ogc.harvard.edu/pages/copyright-and-fair-use#:~:text=Fair%20use%20is%20the%20right,law%20is%20designed%20to%20foster.
[43] "U.S. Copyright Office Fair Use Index," U.S. Copyright Office, February 2025, https://www.copyright.gov/fair-use/#:~:text=Fair%20use%20is%20a%20legal,protected%20works%20in%20certain%20circumstances.

- the effect of the use upon the potential market for or value of the copyrighted work.

In the 2019 Kim Kardashian deepfake parodic video, which utilized a small portion of her real-life Vogue interview, the video was swiftly removed from YouTube by Condé Nast's complaint via the Digital Millennium Copyright Act. Despite the deepfake actually passing the doctrine's cumulative tests, and thus should not have been taken down for copyright infringement.[44]

Further, fair use would still apply, even on the basis of the person's publicity rights. In *Cardtoon v. Major League Basketball Players Association*,[45] the transformative use of the players' faces in the caricature trading cards was found permissible under fair use even if the company was generating profit from it. The court reasoned, (1) substantial transformative parodic elements were added, making the card an entirely new product; (2) no irreparable harm was done to the celebrity's earnings that would outweigh the FOE.[46] While implementation remains slightly flawed, this doctrine balances the protection of personality rights and FOE in digital sphere with its flexible applicability.

## 2. Singapore's Reliance on the Existing Legal Framework before Malignant Deepfakes

Although Singaporeans have adopted more liberal views in certain areas, Singapore's political and legal framework remains relatively conservative compared to the US, especially regarding FOE;[47] a term closely associated with AI. Nonetheless, Singapore is one of the most AI-ready jurisdictions in Southeast Asia and globally.[48] Even without AI legislation like the EU AI Act, Singapore's existing digital legislations, such as, Personal Data Protection Act, Protection from Harassment Act (POHA), Penal Code, and more, demonstrate AI readiness.[49] Here, pertaining to identity theft and NCII deepfakes, the Penal Code and POHA will be analysed respectively.

### A. Singapore's Extensive Protection against Identity Theft

Safeguards against identity theft with non-economic harms can be found systematically within the Penal Code and POHA. The Penal Code Section 416A criminalizes physical or online impersonation under the term 'cheating by personation', where a person pretends to be someone, or knowingly substitutes a person, or misrepresents themselves or any person. The offence exists regardless of the real or imaginary nature of the impersonation subject, with a maximum five-year imprisonment and/or fines.[50] Besides this Code, POHA furthers the protection by prohibiting acts of intentionally causing harassment, alarm or distress to another person through threatening, abusive or insulting behavior, communication or publishing of any identity information of the target person or a related person of the target person. It also criminalizes behaviors and communications which cause fear, provocation or facilitation of violence on the victim.[51] Victims of such impersonation harassment can also apply for a 'Protection Order' or an 'Expedited Protection Order', prior to the court proceeding.[52]

### B. Comprehensive and swift recourse framework for NCII deepfakes

While celebrities may claim protection from NCII deepfakes with copyrights or publicity rights, these

[44] Tiffany C. Li, "Kim Kardashian vs. Deepfakes", Slate, (June 18, 2019), https://slate.com/technology/2019/06/deepfake-kim-kardashian-copyright-law-fair-use.html.
[45] Cardtoons, L.C. v. Major League Baseball Players Association, 95 F.3d 959-62 (10th Cir. 1996).
[46] Andrew Koo, "Right of Publicity: The Right of Publicity Fair Use Doctrine - Adopting a Better Standard", 4 Buff. Intell. Prop. L.J. 1 (2006), p.23-24.
[47] Justin Ong, "Singapore still conservative on moral, sexuality issues, but more liberal since 2002: IPS survey", The Straits Times, (February 03, 2021). https://www.straitstimes.com/singapore/community/singapore-still-conservative-on-moral-sexuality-issues-but-more-liberal-since.
[48] Jason G. Allen, Jane Loo, and Jose Luna. "Governing intelligence: Singapore's evolving AI governance framework" (January 2025). p.2. https://ink.library.smu.edu.sg/sol_research/4569.
[49] "Criminalisation of the Creation or Possession of Sexually Explicit Deepfake Images and Videos", Ministry of Home Affair, (February 05, 2025). https://www.mha.gov.sg/mediaroom/parliamentary/criminalisation-of-the-creation-or-possession-of-sexually-explicit-deepfake-images-and-videos/.
[50] Singapore, Penal Code 1871, (revised, 1 December 2021) §416-417.
[51] Singapore, Protection from Harassment Act 2014, (revised, 1 December 2021), §3-5.
[52] Ibid., §12-13.

are not exactly well-fitted, as harms lie not only in commercial exploitations, but rather in the personality rights themselves. It harms ordinary citizens the same way it does to public figures, because essentially it violates these fundamental rights, regardless of the commercialization.[53]

While acknowledging the Penal Code's applicability to NCII deepfakes, Singapore still indicated plans to amend the Code for better conveyance.[54] Penal Code Section 377BD criminalizes the possession or access of an image or recording of another person with knowledge or reasons to believe that it was done non-consensually, or is likely to cause humiliation, alarm or distress to the person depicted.[55] Much like online impersonation, NCII deepfakes can cause harassment and emotional distress, making POHA provisions also applicable.[56] Currently, Singapore is also establishing a new legislation and agency to enable faster recourse for victims of online harms (including deepfakes), which may mandate a removal timeframe of 24 hours.[57]

# IV. Targeted Amendments for a More Comprehensive Framework

Preceded by the EU AI Liability Directive withdrawal on February 11, 2025,[58] and other Southeast Asian regulatory examples favoring National AI strategies or policy guidelines, there is a present inclination toward bypassing the establishment of a separate AI Code.[59] Instead, states rely on directives or amendments to existing digital laws to counter these emerging threats. From the comparative insights, relevant effective solutions are identified as follows:

- **Identity theft in online impersonation:** The amendment and inclusion of an identity theft provision within the 'Criminal Code', which covers non-economic harms (*i.e. harassments, stalking, stealing of personally identifiable information, etc.*), and a comprehensive framework for victims to swiftly halt the harms, and seek remedies for their tangible and intangible losses from the violation.

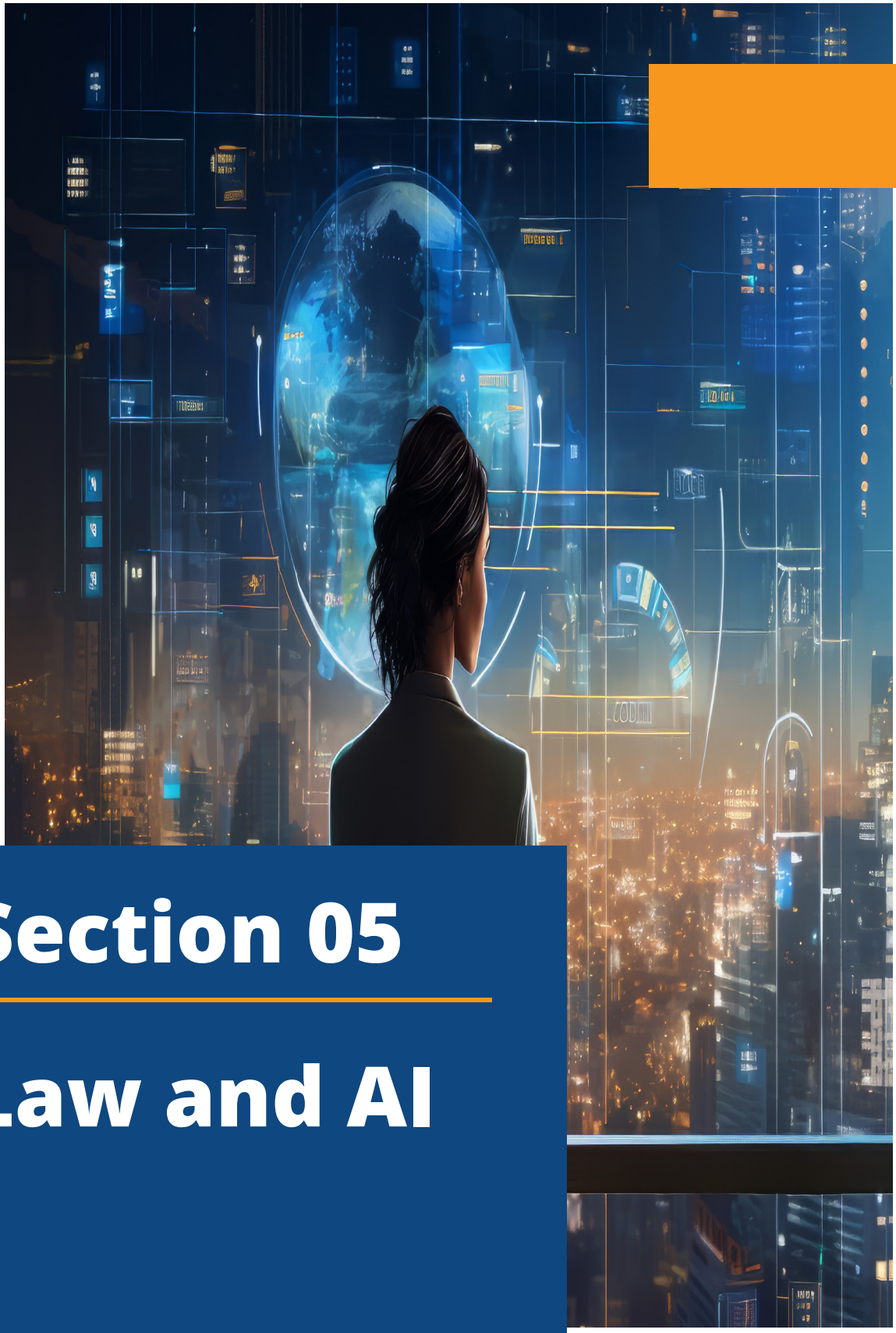
- **NCII deepfakes:** Amendment on the LSHTSE, explicitly criminalizing NCII (real or deepfakes), and identifying victims' remedies for any tangible or intangible losses from the violation, especially for emotional distress and honor or reputation. Additionally, designate an authority agency for victim reporting to prevent secondary victimization. As well as mandate platform providers to remove original content while also making reasonable efforts to take down its duplicates within an appropriate timeframe (ideally, 48 hours). To incentivize platform cooperation, designated authorities may impose fines and tortious liabilities for the lack of reasonable effort in halting the damages.

[53] Sindhu. A, Interventions on the issue of Deepfakes in Copyright, Christ University (2023): pp.1-3. https://www.wipo.int/about-ip/en/artificial_intelligence/conversation_ip_ai/pdf/ind_a.pdf.
[54] Singapore Ministry of Home Affairs, "Criminalisation of the Creation or Possession of Sexually Explicit Deepfake Images and Videos," (February 5, 2025), https://www.mha.gov.sg/mediaroom/parliamentary/criminalisation-of-the-creation-or-possession-of-sexually-explicit-deepfake-images-and-videos/.
[55] Singapore, Penal Code 1871, §377BD.
[56] Singapore, Protection from Harassment Act 2014, §3-4
[57] Osmond Chia, "Victims of Online Harms in Singapore to Get Faster Recourse through One-Stop Government Agency", (October 2, 2024), https://www.straitstimes.com/singapore/victims-of-online-harms-in-singapore-to-get-faster-recourse-through-one-stop-government-agency.
[58] Caitlin Andrews, "European Commission withdraws AI Liability Directive from consideration", IAPP, (February 12, 2025). https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration.
[59] Dr. Richard Sentinella & Joe Jones, "Global AI Law and Policy Tracker", IAPP , (October 2024), p.21. https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf.

# V. Conclusion

Overall, this brief focuses on the interpretation and implications analysis of legislation in domestic and foreign jurisdictions. These findings indicate a need for a tailored and holistic approach for the Cambodian legal framework to incorporate violations of the personality rights in identity theft and NCII deepfakes with swift and comprehensive recourse and redress mechanisms, while upholding FOE commitments under the ICCPR. Nonetheless, there exist constraints within this brief, where further evaluations on other relevant malignant deepfake usages and certain regulation effectiveness are ideal. Within the confines of its scope, this brief sought to holistically address relevant legal vulnerabilities Cambodia faces before deepfakes.

Lastly, these findings could hopefully be the basis of future discussions on the legal implications of Generative-AI and the development of more holistic legal solutions for these problems without compromising the FOE, essential for further innovation and the survival of democracy.



# Section 05

# Law and AI

# Future of AI Liability Regulation in Cambodia: Insights from the Implications of the European Union's Withdrawal of the AI Liability Directive


## SON Solita

[Officer at the Council for the Development of Cambodia]

Son Solita holds a LLB from the Royal University of Law and Economics and a Bachelor of Arts in International Relations from the Royal University of Phnom Penh, enriched by an academic exchange experience at Universitas Airlangga, Indonesia. In addition to her professional role, she has participated in various moot court competitions and academic activities includes KAS-CICP Young IR Scholars Program and KASFLY Fellow 2025.


# I. Introduction

The rapid advancement of Artificial Intelligence (**AI**) has brought unprecedented opportunities for innovation, efficiency, and economic growth. It has also introduced complex legal and ethical challenges, particularly concerning liability, and subsequently the question of who is responsible when AI systems cause harm.[1] The European Union (**EU**), has been at the forefront in AI governance, most effort notably through its regulatory framework, EU's AI Act, which classifies and regulates AI systems based on risk levels while imposing stringent compliance requirements.[2] In a significant and unexpected policy shift, however, the EU has introduced AI Liability Directive (**AILD**) in 2022 but subsequently withdrew the proposal in February 2025,[3] signaling a pivotal reassessment of AI liability mechanisms. This withdrawal raises critical questions about the feasibility of ensuring legal accountability in an AI-dominated landscape, particularly in the absence of a cohesive international liability framework.

While the EU faces challenges in adapting its liability frameworks to the rapid advancement of AI, developing countries like Cambodia also encounter

[1] Sokhean Ben. "Responsible AI: Cambodia Accelerates Efforts on Governance and Ethical Use." Khmer Times, 2023. https://www.khmertimeskh.com/501575910/responsible-ai-cambodia-accelerates-efforts-on-governance-and-ethical-use/.
[2] Meltem Chadwick, Ole Rummel, and Ayse Sungur, "The European Union's Artificial Intelligence Act: Reshaping the Future of Artificial Intelligence Regulation." The SEACEN Centre, 2025, https://suara.seacen.org/the-european-unions-artificial-intelligence-act-reshaping-the-future-of-artificial-intelligence-regulation/.
[3] Datta Anupriya, Theophane Hartmann, and Anupriya Datta. "Commission Withdraws AI Liability Directive After Vance Attack on Regulation." Euractiv, February 12, 2025. https://www.euractiv.com/section/tech/news/commission-withdraws-ai-liability-directive-after-vance-attack-on-regulation/.

significant difficulties in keeping pace with these technological changes.[4] The absence of clear legal definitions and standards specific to AI liability creates uncertainty for courts and regulators, who lack guidance on how to establish fault or negligence in cases involving autonomous or learning AI systems.[5]

Therefore, this paper will explore the implications of the EU's AI Liability Directive withdrawal and examines Cambodia's current legal framework on AI. By analyzing the shortcomings of the EU's experience, this paper seeks to draw lessons that can inform Cambodia's efforts in developing its own AI liability regulations, assessing how these insights could contribute to a more effective and contextually appropriate legal framework, with a focus threshold of AI Liability, allocating the Burden of Proof in AI-Related Liability, adapting Cambodia's legal framework for AI Liability.

# II. From Proposal to Withdrawal of the EU AI Liability Directive

The AILD was proposed to European Commission (**EC**) in September 2022 with the primary aim to address damages caused by AI systems, ensuring victims had access to compensation.[6] Despite initial support, the proposal faced significant opposition from multiple stakeholders, including member states, European Parliament's Internal Market and Consumer Protection Committee (**IMCO**), and industry representatives. Consequently, the EC decided to withdraw the AILD, stating that there is "no foreseeable agreement" on their Work Programme paper, presented on 11 February, 2025.[7] The withdrawal is driven the fundamental concerns about overregulation,[8] enforcement hurdles,[9] and unintended barriers to innovation.[10]

## 1. Overregulation Challenges from the Burden of Proof

Nevertheless, several legal concerns led to its eventual withdrawal. First, there is the challenge of adapting traditional liability principles (the burden of proof) to the context of AI system liability.[11] The proposed directive aimed to modernize liability rules by easing the burden of proof for claimants harmed by AI, introducing a rebuttable presumption of causality that shifts the legal burden to AI developers and operators.[12] However, critics argued that this approach risked undermining legal certainty and fairness.[13] For example, AI systems often operate in complex, non-linear ways that make causal links between action and harm difficult to establish, especially when decision-making is autonomous or based on machine learning models that lack explainability.[14] The AILD's attempt to reverse the burden of proof was seen as potentially clashing with the defendants, particularly businesses that deploy AI but may not have full control over its outcomes.[15]

## 2. Enforcement Challenges

[4] Sokhean Ben. "Responsible AI: Cambodia Accelerates Efforts on Governance and Ethical Use." Khmer Times, 2023. https://www.khmertimeskh.com/501575910/responsible-ai-cambodia-accelerates-efforts-on-governance-and-ethical-use/.
[5] Ibid.
[6] European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), September 28 2022, COM(2022), 496 final https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0496.
[7] Datta Anupriya, Théophane Hartmann, and Anupriya Datta. "Commission Withdraws AI Liability Directive After Vance Attack on Regulation." op.cit.
[8] Cynthia Kroet, "Lawmakers Reject Commission Decision to Scrap Planned AI Liability Rules," Euronews, 2025, https://www.euronews.com/next/2025/02/18/lawmakers-reject-commission-decision-to-scrap-planned-ai-liability-rules.
[9] Ibid.
[10] Kroet, Cynthia. "EU Tech Commissioner Defends Scrapping of AI Liability Rules." Euronews, April 9, 2025, https://www.euronews.com/next/2025/04/09/eu-tech-commissioner-defends-scrapping-of-ai-liability-rules.
[11] Ebers Martin, "Liability for Artificial Intelligence and EU Consumer Law." Journal of Intellectual Property, Information Technology and Electronic Commerce Law 11, 2021, pp. 50–56.
[12] Philipp Hacker, "Explanatory Memorandum of the Proposal for a AI liability directive", 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0496
[13] Cynthia Kroet, "Lawmakers Reject Commission Decision to Scrap Planned AI Liability Rules," op.cit.
[14] EU Commission, "Explanatory Memorandum of the Proposal for a AI liability directive", 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0496
[15] Ibid.

Second, the adoption of the EU AI Act in May 2024 and the anticipated revision of the Product Liability Directive (**PLD**) raised questions about the necessity of the AILD.[16] The EU AI Act Articles 8, 13, and 14 introduce a risk-based regulatory framework that imposes strict requirements on high-risk AI systems to ensure their safety, transparency, and accountability before market deployment.[17] If an AI system fully complies with the AI Act's safety and transparency requirements, the system provider can demonstrate adherence to regulatory obligations, potentially limiting liability under the AILD.

Another significant concern involved the compatibility of the directive with existing national liability frameworks across the EU such as PLD. Some jurisdictions feared that AILD would override or conflict with existing PLD, leading to legal uncertainty rather than clarity.[18] The EU's existing PLD establishes a framework holding producers strictly liable for damage caused by defective products.[19] AI systems often exist as software or cloud-based,[20] blurring the line between "product" and "service." For example, an AI algorithm embedded in a medical device might be considered part of a product,[21] but a cloud-based AI recommendation system may not clearly fall within the PLD's scope. This ambiguity complicates whether AI-related harms can be effectively addressed under which

### 3. Thresholds for Liability

Additionally, the withdrawal was partly driven by debates over the thresholds for accountability, particularly the balance between innovation and protection. Industry groups strongly opposed the proposal, arguing that it would impose overly stringent requirements that could stifle AI innovation.[22] These groups were concerned that the high-risk AI provisions, such as the shifting of the burden of proof and strict liability, would create regulatory burdens that could hinder technological advancement and competitiveness.[23] Moreover, industry groups argued that imposing liability requirements on AI systems with little regard for the complexity of autonomous behavior could result in the misallocation of responsibility.[24] For instance, it would be challenging to determine whether a failure was due to a developer's error, a flaw in the training data, or the misuse of the AI technology by users.[25] The strict nature of the liability rules was seen as disproportionately.

# III. Cambodia's Legal Framework and Gaps in AI Liability

Cambodia's current legal framework does not explicitly address AI liability, but several existing laws and emerging drafts contain relevant principles that can serve as foundational references. The Cambodian Civil Code, enacted in 2007, establishes general tort liability, stating that individuals or entities responsible for causing damage to others due to intentional or negligent conduct must provide compensation.[26] However, this general rule does not specifically address the unique characteristics of AI technologies, particularly their autonomy, unpredictability, and capacity for self-learning, which complicate assigning clear legal liability.

[16] Laura Lazaro Cabrera, Center for Democracy and Technology, "Joint Civil Society Open Letter on the Withdrawal of the AI Liability Directive" Center for Democracy and Technology, 2025. https://cdt.org/insights/joint-civil-society-open-letter-on-the-withdrawal-of-the-ai-liability-directive/#:~:text=The%20withdrawal%20of%20the%20AILD,fairness%2C%20and%20foster%20sustainable%20innovation.
[17] EU Artificial Intelligence Act, 2024, Art. 8, 13 &14.
[18] Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act." op.ci., pp. 97–112.
[19] EU Product Liability Directive, 85/374/EEC, 1985, Art. 1.
[20] Angesh Singh, "Cloud Computing Vs AI - Key Differences Explained!", Digital Regencys,2024, https://www.digitalregenesys.com/blog/cloud-computing-vs-artificial-intelligence.
[21] EU Product Liability Directive, 85/374/EEC, 1985, Art. 2.
[22] Industry Coalition Calls for Withdrawal of AI Liability Directive. 2025, https://www.medtecheurope.org/wp-content/uploads/2025/01/final-aild-joint-statement.pdf.
[23] Ibid.
[24] Ibid.
[25] Neil Sahota, "Who Is Responsible for AI Mistakes? Negligence and AI'S Human Users,", 2024, https://www.neilsahota.com/who-is-responsible-for-ai-mistakes-negligence-and-ais-human-users/.
[26] Cambodian Civil Code (hereinafter called CC), NS/RKM/1207/030, 2007, Art. 743.

Similarly, Cambodia's Law on Consumer protection, designed primarily for human-driven acts and physical goods and services,[27] are ill-equipped to address the unique characteristics of AI, including its unpredictability. Moreover, Prakas on Information Standards for Consumer also mandates that producers and suppliers ensure the safety and quality of their products and services, holding them accountable for harm arising from defects, yet it doesn't not cover the AI goods and services.[28] While this Law and Prakas effectively governs traditional consumer goods, their applicability to sophisticated AI products remains uncertain.

The Law on Telecommunications, introduced in 2015, primarily governs telecommunication services and mandates providers to uphold user data privacy, confidentiality, and quality service standards.[29] Although this law addresses matters related to data privacy and security, it does not explicitly define liability scenarios involving AI systems.

Moreover, Cambodia's draft Law on Personal Data Protection proposes comprehensive guidelines regarding the collection, processing, storage, and sharing of personal data, emphasizing transparency, accountability, and consent mechanisms.[30] These principles are especially pertinent to AI technologies due to their intensive data usage. Nevertheless, this draft law currently does not explicitly provide guidance on liability in situations where AI systems independently infringe data privacy rights or mismanage personal information.

Considering these legislative contexts and gaps, it is crucial for the Cambodia government to proactively address the growing importance and complexity of AI by formulating clear, dedicated AI liability regulation. Drawing inspiration from international frameworks or other countries would help Cambodia adopt a comprehensive, risk-based liability framework specifically tailored to AI technologies.

# IV. Cambodia's First Step Toward AI Liability

As Cambodia's existing legal framework does not explicitly address AI liability, it is crucial to explore how the country might take its first steps in incorporating AI liability into its legal system in the future. Cambodia is likely to encounter several significant challenges in this process, many of which can be informed by lessons learned from the EU's experience with the withdrawal of the AILD.

## 1. Threshold of AI Liability

One of the critical challenges is how to define legally binding thresholds for liability. The EU's experience proves instructive as its initial proposal for strict liability faced fierce opposition from industry groups who argued it would stifle innovation.[31] This tension between ensuring responsibility and fostering growth is particularly acute for Cambodia to navigate these complexities while building its AI liability regulation.

Nevertheless, Singapore has adopted a balanced approach that fosters innovation while safeguarding consumer interests in AI. Rather than imposing blanket liability rules, it has developed targeted

[27] Law on Consumer Protection (hereinafter called LCP), NS/RKM/1119/016, 2019, Art. 3 & 4.
[28] Prakas on Information Standards for Consumer, No.185 P.N. A.KBB.PRK, 2020, Art. 8.
[29] Law on Telecommunication, NS/RKM/1215/017, Art. 64, 65(b),
[30] Draft Law on Personal Data Protection, November 27, 2024, Art. 1.
[31] Industry Coalition Calls for Withdrawal of AI Liability Directive. 2025, https://www.medtecheurope.org/wp-content/uploads/2025/01/final-aild-joint-statement.pdf.

guidelines for high-impact industries like finance and healthcare through its Model AI Governance Framework.[32] The country employs regulatory sandboxes (AI Verify, an AI governance testing framework and a software toolkit) to test AI applications in controlled environments, allowing for real-world evaluation of risks and liability mechanisms.[33] Singapore also emphasizes transparency, requiring documentation of AI decision-making processes to clarify liability when issues arise.[34] This flexible approach enables policy adjustments while maintaining clear accountability standards tailored to different risk levels.

Establish a robust AI liability framework by adopting a multi-layered, adaptive approach could be the best solution to tackle the balanced innovation and protection in Cambodia context. At the foundation, Cambodia would benefit from implement sector-specific liability guidelines involving risk-based categorization, with strict liability for high-stakes applications like healthcare AI and more flexible standards for low-risk commercial uses. This tiered structure should be complemented by mandatory transparency protocols, requiring AI developers to maintain comprehensive documentation of training methodologies, data sources, and decision logic with the purpose of shared responsibility among developers, deployers, and operators. The risk-based structure creates natural incentives for developers to properly assess and mitigate risks, as liability exposure directly correlates with an application's potential harm.

## 2. Allocating the Burden of Proof in AI-Related Liability

Another challenges that would emerge when introducing AI liability regulations in Cambodia context is the difficulty of clearly defining responsibility in AI-related harm cases and who bear the burden of proof.  AI systems often involve multiple stakeholders includes developers, deployers, data providers, and end-users, making it legally complex to determine liability when something goes wrong.[35] This lack of legal clarity could result in either overly broad liability rules on AI developer or leaving victims without proper compensation.

The EU's experience demonstrates that a blanket reversal of the burden of proof onto companies can create excessive litigation risks and stifle innovation, especially for smaller enterprises.[36] The primary issue was that such a blanket reversal would force companies to spend significant resources on legal defense and compliance documentation for every potential claim, regardless of merit.[37] The uncertainty around what constitutes sufficient proof of non-fault in opaque AI systems made the proposal difficult to implement in practice for both larger companies and Small-Medium Enterprises (**SMEs**).[38] This experience suggests that an undifferentiated approach to the burden of proof can disproportionately impact smaller players.

Under Singapore's AI governance framework, particularly the Model AI Governance Framework and subsequent AI Verify initiative, the evidentiary requirements are tailored to the risk level and context of AI deployment rather than applying uniform standards. For high-risk AI applications in regulated

[32] "Singapore's Approach to AI Governance." Personal Data Protection Commission (PDPC), 2020. https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework.
[33] Ibid.
[34] Grayson Chng Darren, and Joe Jones. "Global AI Governance Law and Policy: Singapore." International Association of Privacy Professionals, February 2024. https://iapp.org/resources/article/global-ai-governance-singapore/.
[35] Patrick Upmann, "Who Is Accountable When an AI System Makes Erroneous Decisions That Cause Harm?," AIGN, 2024, https://aign.global/ai-ethics-consulting/patrick-upmann/who-is-accountable-when-an-ai-system-makes-erroneous-decisions-that-cause-harm/.
[36] Jeremy Werner, "European Parliament Committee Opposes AI Liability Directive, Citing Innovation Risks," BABL AI, 2025, https://babl.ai/european-parliament-committee-opposes-ai-liability-directive-citing-innovation-risks/.
[37] Michèle Dubrocard, "AI Liability Rules: A Blocked Horizon?," European Area of Freedom Security & Justice, 2025, https://free-group.eu/2025/03/13/ai-liability-rules-a-blocked-horizon/.
[38] Tambiama Madiega, Briefing: Artificial intelligence liability directive, p.8. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

sectors like finance, compliance with Singapore's Fairness, Ethics, Accountability, Transparency Principles, which the companies are expected to maintain rigorous documentation and audit trails, effectively shifting some burden of proof onto developers to demonstrate compliance with safety and fairness standards if challenged.[39] The Personal Data Protection Act (**PDPA**) further supplements this framework, imposing obligations on AI developers to maintain proper records.[40] These records can be used as evidence in liability claims.[41] This approach also benefits to the plaintiffs as they do not need to understand or reconstruct complex algorithms, as the documentation provided by developers serves as prima facie evidence of harm.

Cambodia would be wise to learn from this by considering more nuanced approaches, such as applying reversed the burden of proof only to clearly defined high-risk. Rather than imposing a uniform standard that shifts the entire evidentiary burden to companies, a more nuanced solution would involve implementing tiered evidentiary rules based on application risk levels. For lower-risk applications, traditional liability principles should apply, with plaintiffs bearing the initial the burden of proof. An intermediate approach could require plaintiffs to first present prima facie evidence of harm before shifting the evidentiary burden to defendants to prove their systems were properly designed and implemented. This approach would also allow for judicial discretion in complex cases where the appropriate standard may not be immediately clear, providing necessary flexibility as the technology continues to evolve. Furthermore, clarifying contractual liability is essential to ensure liability actor. A balanced approach could follow that deployers bear primary liability for harms caused by AI applications, unless negligence or misconduct by developers. However, contracts between developers and deployers should explicitly outline responsibilities to determine whether liability should shift back to developers in cases of defective algorithms, biased training data, or failure to disclose known risks.

## 3. Adapting Cambodia's Legal Framework for AI Liability

As Cambodia in the process of developing its AI legal framework, a crucial consideration is whether to establish a standalone AI liability framework or integrate AI-related liability provisions within the existing legal system. The withdrawal of the EU's AILD offers an important lesson about the challenges of establishing standalone AI liability frameworks. A key factor was concerns about regulatory overlap, as many of its proposed obligations were already addressed by existing legal instruments, particularly the EU AI Act and the revised Product Liability Directive.

In contrast, Singapore and Japan have adopted more integrated approaches that align AI governance with their broader legal systems. Singapore, with its Model AI Governance Framework and sector-specific regulations, has ensured that AI liability is addressed within the context of existing legal act.[42] Similarly, Japan has taken an initial approach by amending existing laws rather than creating new AI-specific liability rules. The cornerstone of this process is the 2023 amendment to Japan's Consumer Contract Act, which protects consumers from unfair AI-driven contracts or deceptive AI services.[43] Simultaneously, Japan has made targeted amendment to its Civil Code in 2020 to clarify liability attribution for autonomous AI actions.[44]

[39] Monetary Authority of Singapore (MAS), Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector, 2018, https://www.mas.gov.sg/-/media/mas/news-and-publications/monographs-and-information-papers/feat-principles-updated-7-feb-19.pdf.
[40] Personal Data Protection Commission (PDPC), Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems, 2024, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf
[41] Ibid.
[42] Personal Data Protection Commission (PDPC). Overview of PDPA. https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act.
[43] Ikeda, Junichi, Takayuki Fujii, Hiroki Hagihara, Mai Nishigori, and Nagashima Ohno & Tsunematsu. "Product Liability & Safety 2023." CHAMBERS GLOBAL PRACTICE GUIDES, 2023. https://www.noandt.com/wp-content/uploads/2023/07/cp_gpg_product_liability_2023_1.pdf.
[44] Japan Civil Code, art. 709.

# V. Conclusion

The evolving landscape of AI presents significant challenges for legal systems worldwide, including Cambodia, in terms of liability regulation. The EU's withdrawal of the AILD highlights critical lessons for Cambodia as it navigates the complexities of AI governance. The EU's experience underscores the difficulties in establishing clear liability frameworks for AI, particularly given the technology's inherent autonomy, unpredictability, and opacity.

For Cambodia, the absence of explicit AI liability provisions in its current legal framework presents both a challenge and an opportunity to develop a comprehensive and adaptive approach. Drawing on international experiences, from the EU, Singapore, and Japan, Cambodia is well-positioned to integrate AI liability into its existing legal framework, avoiding the creation of standalone frameworks that may lead to regulatory overlap. A nuanced, risk-based liability model targeting high-risk sectors while providing more flexibility for lower-risk applications would promote both innovation and consumer protection. This adaptive, comprehensive framework is crucial to ensure Cambodia's legal system remains responsive to the evolving AI landscape.

# Discriminatory Risks of Predictive Artificial Intelligence and Inferences of Sensitive Personal Data: Considerations for Cambodia


## HENG Sirimongkul

[Junior law and economics student, American University of Phnom Penh]

He is the current president of the Raymond Leos Law Society at AUPP. Previously, he was awarded Best Oralist, Best Respondent Memorial, and Co-Champions at the Cambodia National Rounds of the Philip C. Jessup International Law Moot Court Competition 2025.He also founded the AUPP Debate Society and was given the Diplomacy Award by the ASEAN Foundation in the ASEAN Foundation Model ASEAN Meeting Plus Japan 2023.


# I. Introduction

As predictive Artificial Intelligence ("AI") systems are increasingly employed in decision-making and recommendations system, they introduce great possibility for increasing the efficiency of work processes and the economy. It is expected to contribute almost 1 trillion dollars to ASEAN's GDP by 2030.[1] However, there are also increased risks that AI processing of personal data may erode the foundational right to non-discrimination, particularly when it is capable of inferring sensitive personal data from non-sensitive personal data or proxy data. Consequently, this paper will seek to explore (**II**) predictive AI's role in exacerbating discrimination by inferring sensitive data from proxy data, (**III**) define the categorization of sensitive data in the AI processing of personal data, and lastly do (**VI**) a comparative analysis of AI-specific regulation to address the discriminatory risks of AI in the EU and Singapore. Recommendations will be integrated for Cambodia's approach to addressing this sensitive data protection and non-discrimination risks.

[1] McKinsey Global Institute, Artificial Intelligence and Southeast Asia's Future, McKinsey & Company, 2017, 3, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/AI%20and%20SE%20ASIA%20future/Artificial-intelligence-and-Southeast-Asias-future.ashx.

# II. Predictive AI's Role in Exacerbating Discrimination by Inferring Sensitive Data from Proxy Data

## 1. Rationale of Sensitive Data Protection and its Role Against Discrimination

One of the underlying fundamental rights that data protection seeks to uphold is the right to non-discrimination.[2] One of the ways that data protection laws seek to the uphold such right is by recognizing an increased level of protection for sensitive personal data. As Cambodia is in the process of adopting a more comprehensive personal data protection law, its current laws have yet to recognize the sensitivity of certain personal data. However, the Cambodian Constitution may be understood to be the implicit basis behind such recognition. Article 40 recognizes the right to privacy of residence and secrecy of correspondence. While Article 31 enshrines that all individuals are equal before the law without any discrimination based on race, sex, language, beliefs, religions, political tendencies, birth origin, social status, wealth, or other situations.[3] Further, Article 38 also maintains that the law shall protect the life, honor, and dignity of the citizens.[4]

While in the European Union, the General Data Protection Regulation does place a general prohibition on the processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, health and biometric data.[5] These processing are classified as processing of special categories of personal data because they are personal data which are sensitive in nature as they relate to a group characteristic of a data subject whose disclosure would violate their right to privacy and dignityand which may be used maliciously to discriminate and violate the fundamental rights of that subject.[6] Such provision is a manifestation of the protection of one of the fundamental rights of individuals under the European Convention on Human Rights Article 21 on the prohibition of discrimination of individuals based on their group characteristic.[7]

## 2. Challenges of AI and Proxy Data to Sensitive Data Protection

Discrimination is not merely the result of only processing input sensitive data, but rather the output that results from such processing.[8] AI largely expands the horizon for these discrimination risks as its ability to recognize patterns and draw inferences from non-special personal data.[9] These proxy data, such as that of purchasing decisions of the data subject may in aggregate, through the use of predictive artificial intelligence in decision-making and recommendation systems, reveal protected

[2] European Parliament. European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)).P8_TA(2017)0076. Strasbourg, 14 March 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_EN.html.
[3] Kingdom of Cambodia, Constitution of the Kingdom of Cambodia, promulgated 21 September 1993, last amended 2008, art. 31, https://www.constituteproject.org/constitution/Cambodia_2008.
[4] Id., art. 38; Individual rights in the Cambodian Civil Code also enshrines the right to freedom, identity, dignity and privacy. Kingdom of Cambodia, Civil Code of the Kingdom of Cambodia, promulgated 8 December 2007, art. 10, https://moj.gov.kh/files/user-folder/Media-Law/Civil-Law/Law_030_1207_EN.pdf.
[5] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 9(1), Official Journal of the European Union L 119 (May 4, 2016): 38, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[6] Id., Recital 51, ¶ 1; Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, eds., The EU General Data Protection Regulation (GDPR): A Commentary, 2nd ed. (Oxford: Oxford University Press, 2020), 369-370.
[7] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, art. 21
[8] Antoinette Rouvroy, "Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data," Council of Europe, Directorate General of Human Rights and Rule of Law, January 11, 2016, 16-17, https://rm.coe.int/16806a60201.
[9] Pu Chen, Linna Wu, and Lei Wang, "AI Fairness in Data Management and Analytics: A Review on Challenges, Methodologies and Applications," Applied Sciences 13, no. 18 (2023): 10258. https://doi.org/10.3390/app131810258.

attributes such as that of sexual orientation and other details of that subject's private life.[10] In this case, the inferences made by such personal data can infringe upon the private lives of the individuals and can be used in decision-making or recommendation processes, such as that of setting insurance premiums, personalized advertising, or hiring which would produce discriminatory effects against them.[11]

For example, when Amazon used an AI system to numerically assess a pool of candidates based on their resumes, it was found that the system disproportionately disfavors female candidates.[12] The resumes did not explicitly state the candidate's sexual orientation, but the AI system had inferred such protected attribute from the word "women's" or certain women's college contained in the resumes. Based on a previous biased data set that the AI's algorithm was trained on, the algorithm favored giving higher ratings to male candidates. Other proxy data, such as that of the postcodes of the candidate's address, might have also been used to infer their racial or class background.[13] Based on this inference, even when there is no processing of special categories of personal data, the result is likely that there would still be discrimination against these protected attributes.

# III. Defining the Categorization of Sensitive Data in the AI Processing of Personal Data

As shown above, the usage of predictive AI could effectively mean that any type of personal data could be used to infer protected attributes.[14] As this classification of special categories of personal data seeks to uphold the fundamental rights to privacy, dignity, and non-discrimination,[15] this presents a clear issue with the definition of the processing of sensitive personal data, or special categories of personal data.

It may be argued that since the definition for special categories of personal data under Article 9(1) of the GDPR is only that the processing reveals protected attributes, then those inferential processing would be prohibited without explicit consent or other exceptions.[16] However, taking this stance would be ineffective as it would mean that any data could possibly fall into prohibition if the processing is conducted by predictive AI.[17] Given the risks, the following sections will lay out three choices of a test that may be employed to identify sensitive personal by the proposed Cambodia's Personal Data Protection Regulator :[18]

[10] Oboler, A., Welsh, K., & Cruz, L. (2012b). The danger of big data: Social media as computational social science. First Monday, 7. https://www.oboler.com/the-danger-of-big-data-social-media-as-computational-social-science/.
[11] Sandra Wachter, "Data Protection in the Age of Big Data," Nature Electronics 2 (2019): 6, https://doi.org/10.1038/s41928-018-0193-y1.
[12] Erin Winick, "Amazon Ditched AI Recruitment Software Because It Was Biased against Women," MIT Technology Review, October 10, 2018, https://www.technologyreview.com/2018/10/10/139858/amazon-ditched-ai-recruitment-software-because-it-was-biased-against-women/.
[13] Article 29 Data Protection Working Party, Advice Paper on Special Categories of Data ("Sensitive Data"), Ares(2011)444105, April 20, 2011, 6, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.
[14] Paul Quinn and Gianclaudio Malgieri, "The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework," German Law Journal 22, no. 8 (December 2021): 1611, https://doi.org/10.1017/glj.2021.82.
[15] Cf. European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), Recital 51.
[16] Id., art. 9(1).
[17] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," Seton Hall Law Review 47, no. 4 (2017): 995–1020, https://scholarship.shu.edu/shlr/vol47/iss4/2/1.
[18] Kong Phallack, "Developing a Comprehensive Personal Data Protection Framework for Cambodia," in Regulating Personal Data Protection and Privacy: Practical and Legal Considerations for Cambodia and Beyond, KAS The Law Talk Publication, Konrad-Adenauer-Stiftung Cambodia, 2023.

## 1. The reliability test

The reliability test is predicated on whether the processing of those proxy data would create a reliable inference of the protected attributes, or "a statistically significant basis to infer sensitive information".[19] Whether the proxy data would fit in with these criteria would likely have to do with the content of the data.[20] Certain processing would ultimately raise more risks such as photos and images which would be able to reveal race, ethnicity, or health status.[21] Certainly, the jurisprudence of the European Court of Justice affirmed that such processing of personal data will become processing of special categories of personal data if it can reliably be used to predict protected attributes.[22]

The obvious issue with the employment of this reliability test is that the predictive models do not need to be accurate for it to produce harmful effects. The profiling made by these models can have an ability to create "self-fulfilling prophecies".[23] For example, the targeted advertisement of certain products to a certain group of individuals may self-perpetuate the bias that that group of individuals is inclined towards that type of product. As those individuals lack much autonomy over the type of advertisement presented to them, they may resort to purchasing those products, reinforcing the bias.[24]

## 2. The purpose test

The purpose test considers the intended purpose pursued by the data processor, and whether there was intent to reveal protected attributes.[25] The intent may be understood as not just predictive AI correlatively inferring those attributes, but that it is relied upon by recommendation or decision-making system of a data processor. This test seems to be the stance adopted by the United Kingdom's Information Commissioner's Office (**ICO**). In the Cambridge Analytica Scandal, the ICO concluded that processing online activities of Facebook users to make predictions about their political affiliations and opinions can indeed fall under the prohibition of processing of special categories of personal data, even if those inferences may not be entirely accurate.[26]

However, the issue with the employment of this purpose test is that it would be hard for regulators to assess the intended purpose of processing declared by the processor. As such, the processor may not declare its intention to reveal protected attributes even when its intention was to the contrary. Further, even if there were no intention, biased algorithms or negligent processing could still result in inadvertently revealing those attributes.[27]

## 3. The purpose and contextuality test

The purpose and contextuality approach considers both the purpose and the context by which the data is processed as conjunctive determinants to classify sensitive data. Particularly, the contextual element requires "that the specific interests of the controller, as well as of the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the persons involved" be examined.[28]

[19] Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," Columbia Business Law Review 2 (2019): 75.
[20] Douwe Korff, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Working Paper No. 2 (Brussels: European Commission Directorate-General Justice, Freedom and Security, 2010), 41.
[21] Cf. Article 29 Working Party, Advice Paper, 8.
[22] Case T-190/10, Kathleen Egan and Margaret Hackett v. European Parliament, ECLI:EU:T:2012:16, Judgment of the General Court (Second Chamber), 18 January 2012.
[23] Wouter A.C. van Amsterdam et al., "When Accurate Prediction Models Yield Harmful Self-Fulfilling Prophecies," preprint, last revised August 26, 2024, arXiv:2312.01210 [stat.ME], 10–11, https://arxiv.org/abs/2312.01210.
[24] Jeannie Marie Paterson et al., "The Hidden Harms of Targeted Advertising by Algorithms and Interventions from the Consumer Protection Toolkit," International Journal of Consumer Law and Practice9 (2021): 9, https://ssrn.com/abstract=3993496.
[25] Cf. Wachter and Mittelstadt, "A Right to Reasonable Inferences," 77.
[26] Information Commissioner's Office, Investigation into the Use of Data Analytics in Political Campaigns: A Report to Parliament, 6 November 2018, p. 36, https://ico.org.uk/media2/migrated/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.
[27] Quinn and Malgieri, "The Difficulty of Defining Sensitive Data," 1594-1595.
[28] Id., 1591.

Given the previously discussed pitfall with the sole deployment of the purpose test, contextuality in this approach is applied to ensure that there is a prima facie reasonableness assessment of the declaration of purpose by the processor. Consequently, Quinn and Malgieri argue that this test would function as a two-step method. The first step is to determine whether there was intent to reveal protected attributes from processing. If the answer is in the affirmative, then the data would be sensitive. If the answer is in the negative, then the regulator should assess whether the content of the data (e.g. high-risk personal data such as photograph or video recordings) would require it to be assessed contextually. [29]

This two-pronged approach may be desirable rather than purely a reliability test, or a purpose test as it allows for flexibility in regulation, while also ensuring adequate protection against abuse by data processors to circumvent the sensitive data protection.

# IV. Addressing the Discriminatory Risks of Predictive AI through AI-Specific Regulation: Comparative Analysis of EU and Singapore Jurisdiction

Given the complex nature of the implementation of the goals of sensitive data protection with the advent of predictive AI, one could argue that a data protection approach alone is insufficient and that a AI-specific regulation may be necessary. This necessarily indicates a need to address discrimination risks from a societal, and not just an individual point of view, like that of personal data protection laws.[30] This was certainly recognized by jurisdictions like that of the EU with the AI Act, and Singapore through its Model AI Governance Framework. This section will explore how both jurisdictions dealt with the discriminatory risks posed by AI, and make recommendations to Cambodia's approach to AI regulation.

## 1. The EU's AI Act

Th EU's AI Act sought to fill some of the regulatory gap by imposing obligations on the processors to ensure that such inferences from AI deployment is fair, transparent and explainable.[31] The Act functions on a risk-based system by categorizing AI systems by their level of risks. High-risk AI systems are inter alia systems that pose serious risks to health, safety, or fundamental rights of individuals, including that of non-discrimination.[32] Deployers of high-risk AI systems are obligated to give clear instructions as to their intended usage, level of accuracy in the output, and transparency regarding how it arrived at the ouput if applicable.[33] The Act also obligates the need for effective human oversight for such high-risk AI systems.[34] These are separate governing obligations on the usage of AI for

[29] Id., 1609-1610.
[30] Jennifer King and Caroline Meinhardt, Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World (Stanford, CA: Stanford HAI, 2024), 19–21, https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information.
[31] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Regulations and Directives (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, July 12, 2024. Article 13-14, 50. Accessed June 14, 2025. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
[32] Article 6 as a whole defines what a High-Risk AI System is, by referring to specific annexes of the EU AI Act particularly Annex I and Annex III. Id., art. 6; For discussion see Holistic AI Team, "High-Risk AI Systems Under the EU AI Act," EU AI Act, https://www.euaiact.com/blog/high-risk-ai-systems-under-the-eu-ai-act.
[33] Id., arts. 13-14, 50.
[34] Id., art. 14.

the AI deployers/data processors in addition to compliance with the GDPR.[35] Failure to comply with these obligations would result in severe penalties similar to a breach of the GDPR.[36]

Such hard AI regulation is unlikely to be adopted anytime soon in Cambodia, as the technology has yet to be widely adopted in Cambodia,[37] and is viewed to be largely constraining on developing countries.[38] However, the risks posed by the usage of such AI systems are still pertinent as businesses, employers, banks and other entities are already considering the usage of AI to faciliate their work.[39] Recent developments in the drafting of the Cambodia's National AI Strategy.[40] Indicates its stance against adopting the EU's approach but rather to adopt a soft-law approach like that of Singapore. The document's Strategic Priority 5 emphasizes strategic measures to develop non-binding principles of ethical and responsible development, deployment, and use of AI. Nevertheless, the AI Act offers some useful guiding principles on AI deployment which Cambodia's proposed Personal Data Protection Regulator could encourage data processors, who use AI, to structure their deployment, particularly the principle of fairness, transparency, and explainability of AI systems.

## 2. Singapore's Model AI Governance Framework

The Singapore Model has been praised for its innovativeness in shaping the ethical and responsible use of AI without stifling innovation and deployment.[41] Its Model AI Governance Framework introduces non-binding guidelines and recommendations on the ethical and responsible deployment of AI systems.[42] Further, there are sectoral guidelines that are issued by each competent authority,[43] that seek to regulate those sectors' deployment of AI more specifically. For example, the Monetary Authority of Singapore sets out guidelines in 2018 on fair, ethical, accountable, and transparent usage of AI in the financial sector.[44] Likewise, Cambodia may consider adopting sectoral guidelines on AI deployment, such as a guideline for the banking sector by the National Bank of Cambodia, a guideline for the telecommunications sector by the Telecommunication Regulator of Cambodia, etc. In addition to this, Singapore also introduces a certification system for AI models called AI Verify to assess the compliance of AI models with its internationally accepted AI ethics principles.[45]

To ensure that AI deployment is compliant with the upcoming personal data protection law, Cambodia may adopt this certification approach to induce voluntary compliance with its ethical and responsible AI use principles. In addition, Cambodia may also consider developing an advisory guideline on data protection for AI systems, similar to Singapore's Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems,[46] to further this goal.

[35] Id., article 2(7).
[36] Id., arts. 99-101.
[37] Taing Rinith, "Cambodia's AI Journey: Overcoming Challenges to Harness Advanced Tech," Khmer Times, accessed June 16, 2025, https://www.khmertimeskh.com/501597302/cambodias-ai-journey-overcoming-challenges-to-harness-advanced-tech/.
[38] Mona Nabil Demaidi, Artificial Intelligence National Strategy in a Developing Country, AI & Society 40 (2025): 433, https://doi.org/10.1007/s00146-023-01779-x.
[39] Ministry of Industry, Science, Technology & Innovation (Cambodia), AI Landscape in Cambodia: Current Status and Future Trends, May 30, 2023, https://misti.gov.kh/public/file/20230530168542628 5.pdf.
[40] Ministry of Post and Telecommunications, Draft National Artificial Intelligence Strategy 2025–2030, June 2025, accessed June 17, 2025, https://www.facebook.com/share/p/192T2iBBTw/.
[41] Sudeep Khanal, Hongzhong Zhang, and Ali Taeihagh, "Building an AI Ecosystem in a Small Nation: Lessons from Singapore's Journey to the Forefront of AI," Humanities and Social Sciences Communications 11, no. 1 (2024): 866, https://doi.org/10.1057/s41599-024-03289-7.
[42] Personal Data Protection Commission. Model AI Governance Framework. Singapore: PDPC, January 2020. https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework; For its Framework on Generative AI see Infocomm Media Development Authority and AI Verify Foundation. Model AI Governance Framework for Generative AI. Singapore: IMDA, January 2024. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai.
[43] Joe Jones and Darren Grayson Chng. Global AI Governance Law and Policy: Singapore. International Association of Privacy Professionals (IAPP), February 2024. https://iapp.org/resources/article/global-ai-governance-singapore/.
[44] Monetary Authority of Singapore. Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. Singapore: MAS, November 2018. https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf.
[45] Josh Lee Kok Thong, Singapore's AI Governance Journey: Ethical, Social and Regulatory Considerations, presentation at KAS Special Lecture, March 1, 2025, Google Drive, https://drive.google.com/file/d/1aLC6y3FyetWN1slRQoEHJlqQUn2JwncL/view?usp=share_link.
[46] Personal Data Protection Commission. Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems. Singapore: PDPC, March 1, 2024. https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf.

These quasi-regulations serve to influence businesses to comply with industry and government-accepted standards on the ethical and responsible deployment of AI.[47] This approach seems to be more in line with Cambodia's current stage of AI adoption, as it focuses on voluntary compliance, which offers flexibility for regulation to evolve with industry best practices to ensure that any AI-specific regulation does not become obsolete due to the fast-changing nature of the technology.

# V. Conclusion

In conclusion, predictive AI presents an insiduous risk in undermining the fundamental right to non-discrimination due its ability to infer sensitive data or protected attributes from proxy data. In order to tackle this issue, regulators should define the categorization of sensitive data in the context of AI processing by considering either the reliability, the purpose, or the purpose and contextuality test. Additionally, an AI-specific regulation in the form of a soft-law akin to Singapore's approach may be more applicable to the Cambodian context than the EU's AI Act in mitigating the discriminatory risks and ensuring compliance with ethical and responsible principles for AI deployment.

[47] J. Soh, L. Lim, and Z. K. Yeong, Artificial Intelligence in the Regulatory Wonderland (forthcoming; draft on file with the authors), as cited in Jason Grant Allen, Jane Loo, and Jose Luis Luna Campoverde, "Governing Intelligence: Singapore's Evolving AI Governance Framework," Cambridge Forum on AI: Law and Governance 1 (2025): 6, https://doi.org/10.1017/cfl.2024.12.

KONRAD ADENAUER STIFTUNG

**Konrad-Adenauer-Stiftung, Cambodia**
House No. 4, Street 462, Khan Chamkar Mon P.O.box 944,
Phnom Penh. Kingdom of Cambodia
Telephone : +855 23 966 171
E-mail: Office.Phnompenh@kas.de
Website : www.kas.de/cambodia
Facebook: www.facebook.com/kaskambodscha
Instagram: www.instagram.com/kas_cambodia



សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ
និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច
ROYAL UNIVERSITY OF LAW AND ECONOMICS

**Royal University of Law and Economics**
Monivong Boulevard, District Tonle Bassac,
Khan Chamkamon, Phnom Penh.
Kingdom of Cambodia
Telephone: +855 12 564 094
E-mail : rector@rule.edu.kh
Website: www.rule.edu.kh
Facebook https://web.facebook.com/rule.edu.kh

9 789924 671322