



សាកលវិទ្យាល័យគុយឡីត៍សាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច  
UNIVERSITE ROYALE DE DROIT ET DES SCIENCES ECONOMIQUES  
ROYAL UNIVERSITY OF LAW AND ECONOMICS



KONRAD  
ADENAUER  
STIFTUNG

# LAW AND INNOVATION ECONOMY

LAW BRIEF 2026

## ABOUT KONRAD-ADENAUER-STIFTUNG

Freedom, justice, and solidarity are the basic principles underlying the work of the Konrad-Adenauer-Stiftung (KAS). The 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 in freedom and dignity. We make a contribution underpinned by values to helping 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 economic and social development. All programs are conceived and implemented in close cooperation with the Cambodian partners on central and sub-national levels.

Learn more through: <https://kas.de/cambodia>



**សាកលវិទ្យាល័យក្រុងនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច**  
UNIVERSITE ROYALE DE DROIT ET DES SCIENCES ECONOMIQUES  
ROYAL UNIVERSITY OF LAW AND ECONOMICS

## ABOUT ROYAL UNIVERSITY OF LAW AND ECONOMICS

The Royal University of Law and Economics (RULE) is the first and oldest 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/>

## **ABOUT LAW BRIEF**

It is a compilation of legal articles produced by Konrad-Adenauer-Stiftung For Legal Youth (KASFLY) fellows in the fellowship 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 (RULE), 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 KASFLY**

Since its establishment in 2017, KASFLY 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.

For more information, please contact:

**Mr. TOUCH Rattanakraingsey**  
**Program Manager**  
[rattanakraingsey.touch@kas.de](mailto:rattanakraingsey.touch@kas.de)

ORGANISED IN PARTNERSHIP WITH



សាកលវិទ្យាល័យគ្រូមិនីស្ត្រីសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច  
UNIVERSITE ROYALE DE DROIT ET DES SCIENCES ECONOMIQUES  
ROYAL UNIVERSITY OF LAW AND ECONOMICS

## Law Brief: Law and Innovation Economy

Issued in August 2026

### Edited by

Paul Mornet

Touch Rattanakraingsey

### Editorial Support

Dr. Pan Sophearith

Poeng Somalika

Koeut Sokunkosoma

### Production Team

Touch Rattanakraingsey

Mey Victoria

### Cover Design

Soeun Brosnuth

### Layout Design

Ly Nittavann

### 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.

Published by the Konrad-Adenauer-Stiftung Cambodia

Copyrights © Konrad-Adenauer-Stiftung



**TABLE OF CONTENT**

**FOREWORD.....1**

**EDITOR’S NOTE.....2**

**ABOUT AUTHORS.....3**

**PART 1: DIGITAL SERVICES AND LAW.....5**

**The Dilemma of Labour Protection: Shaping a Legal Status for Platform Workers in Cambodia.....6**  
*KOEUT Sokunpanita*

**Platform Liability and the Digital Accountability Gap: A Legal Analysis of Cambodia’s E-Commerce Regulation.....14**  
*OU Sobandolkalyan*

**Legal Liability for Digital Service Providers in the Transportation Industry.....22**  
*LA Sophavann*

**The Legal Implications of Deferred Equity: Reforming Cambodia’s Legal Framework for Startup Equity Compensation.....29**  
*SE Chhunlim*

**When Digital Data Drives Market Power: Evaluating Cambodia’s Competition Framework for App-Based Mobility Services.....35**  
*NHETH Vichetneath*

**Conditionality in the Formation of Electronic Contracts: Does It Ensure a Fair and Balanced Relationship Between Parties?.....44**  
*HORN Sokngim*

**PART 2: CRIMINAL PROCEDURES IN THE CONTEXT OF CYBERCRIME.....51**

**Digital Evidence Acquisition from Smartphones and Computers in Cambodian Criminal Proceedings.....52**  
*SOMNANG Odom*

**Confiscation of Digital Assets under Cambodian Criminal Proceedings: Procedural Gaps and Enforcement Challenges.....61**  
*YIN Hongleang*

**Cybersecurity Incident Reporting in Cambodia’s Banking Sector: Addressing Regulatory Fragmentation and Institutional Coordination.....69**  
*BON Somrach*

**PART 3: DIGITAL FINANCE AND GREEN FINANCE LAW .....80**

Carbon Credit Trading in Cambodia.....81

*POENG Somalika*

Licensing Foreign Cryptoasset Service Providers In Cambodia: A Legal Analysis of Registration Barriers.....91

*TAING Kimsuo*

**PART 4: ARTIFICIAL INTELLIGENCE, DATA AND LAW .....98**

Artificial Intelligence Training Using Copyrighted Works and Exception of Educational Use.....99

*LENG Chansovannarath*

The Legal Status of Synthetic Data Under Cambodian Law Where Re-Identification Is Reasonably Possible.....108

*HAY Sarkunmealea*

## FOREWORD

Since 2017, the Konrad-Adenauer-Stiftung for Legal Youth Fellowship, better known as KASFLY, has supported successive cohorts of law students and young professionals in developing their research, legal analysis, and writing. Through extensive drafting, discussion, and revision, fellows grew from students into published authors. This final edition, under the theme *Law and the Innovation Economy*, examines whether Cambodia's legal frameworks are keeping pace with rapid technological and economic change. The thirteen briefs identify emerging legal challenges, draw lessons from comparative experience, and offer practical recommendations suited to Cambodia's context.

Part One examines digital services and platform-based business models, including the legal status of delivery and ride-hailing drivers, platform liability, electronic contracts, start-up compensation, and data-driven market power. Part Two considers the challenges that digital evidence, blockchain-based assets, and cyberattack on police investigations, criminal justice, and regulatory enforcement in Cambodia. Part Three addresses two developing markets: carbon credit trading and cryptoasset services. Part Four explores the relationship between artificial intelligence, copyright, synthetic data, and data rights. Across these areas, the authors draw insights from the European Union, Singapore, Malaysia, and Vietnam while considering how international approaches may be adapted to Cambodian conditions.

Although the briefs offer concrete recommendations, they also invite further research, dialogue, and cooperation among lawmakers, legal practitioners, businesses, researchers, and the public. Responsive regulation must protect rights and promote accountability while allowing innovation to support Cambodia's social and economic development. We extend our sincere appreciation to the Royal University of Law and Economics, our longstanding partner, and to the mentors, editors, and reviewers whose guidance strengthened each contribution. Above all, we congratulate the fourteen fellows and authors whose commitment and intellectual curiosity made this publication possible. This edition also marks the final publication of the KAS Cambodia office. KAS will continue contributing to Cambodia through its regional programmes and through the partners, alumni, and friends with whom it has worked since 1994. although office is closing KAS and its wide network together with partner will carry on.

### A word from the Country Director

*"Presenting the final edition of Law Brief is both a proud and reflective moment. Since 1994, KAS has had the privilege of working alongside Cambodian institutions, scholars, policy and law makers, and young leaders. This publication reflects that enduring partnership and the commitment of a new generation of legal thinkers to addressing Cambodia's emerging challenges. The thoughtful analysis and practical recommendations presented by these young authors give me great confidence in the future of Cambodia's legal community. Although this publication marks the conclusion of KASFLY and the closure of the KAS Cambodia office, our relationship with Cambodia will continue through our regional programmes and the network of partners, alumni, and friends built over more than three decades. An office may close, but genuine partnership endures through the people who carry its purpose forward. I warmly congratulate the authors and sincerely thank everyone who has contributed to this remarkable journey."*

### A word from the Program Manager

*"KASFLY is a unique program and community for law students and young professionals, offering specialized training and publication platforms to foster academic growth. It also creates a space where senior legal professionals give back to juniors, participant able to freely express their thought and opinion, and strengthening the foundation of legal field. While this book closes the program, your legal journey is only just beginning. Put what you have learned into the service of your nation, and know that we remain only a message away."*

*To the fellows of 2026, congratulations. You now join a community of KASFLY alumni who practise law, serve in both public and private institutions, contribute to judicial system, and teach the next generation. This publication reflects your hard work and marks the beginning of your continued contribution to Cambodia's legal development. We hope the ideas presented in these pages will stimulate informed discussion, inspire further research, and contribute to a legal environment in which innovation, justice, and responsible development can advance together.*

**Mrs. Natalie Russmann**  
Country Director, KAS Cambodia and Malaysia

**Mr. Touch Rattanakraingsey**  
Program Manager, KAS Cambodia

## EDITOR'S NOTE

It is with a particular emotion that I write this year editor's notes, as the 2026 KASFLY publication will be the last of a decade-long series, which I had the privilege of supervising for the past three years. Fantastic memories were made with KAS colleagues, and of course with the successive generations of brilliant fellows, many of whom grew to become respected lawyers and competent civil servants. I would like to use this opportunity to celebrate what KAS Cambodian office has produced, which was an authentic, unique and needed space, which many of us could call a second home. KAS came all these years in Cambodia with funds (an increasingly rare occurrence), and used them to empower young people, as illustrated in its recruitment policy. This space will be dearly missed, but ardent memories will continue to live on.

This final publication contributes to the important conversation pertaining to the calibration of the legal and regulatory responses to Cambodia's rapid adoption of digital innovations, by shedding light on some of the most pressing legal problems arising from observation of legal gaps, conflicts, derogations or misunderstandings. It is structured in four parts, namely Digital Services and Law, Criminal Procedures in the Context of Cybercrime, Digital Finance Law and Sustainability, and Artificial Intelligence, Data and Law. Each contribution focuses on a narrowly defined legal issue that is both timely and relevant to policymakers, practitioners, businesses, and citizens engaged in this ongoing transformation. Through careful analysis, the authors identify competing legal and policy approaches, examine their respective merits and shortcomings, and ultimately propose solutions adapted to Cambodia's technological, economic, and legal context. Comparative analysis occupies an important place throughout this publication. By examining legislative choices and regulatory experiences from foreign jurisdictions, the authors seek to enrich their reasoning and draw lessons from both successes and shortcomings elsewhere. Particular attention is devoted to the influence of foreign legal systems, notably that of the European Union, whose regulatory approaches have increasingly inspired Cambodian lawmakers and legal practitioners in the digital sphere.

Readers should also bear in mind the particular profiles of the young authors behind these law briefs and the circumstances that led them to devote considerable time and effort to researching these diverse topics. Carefully selected by the KAS FLY team, these young apprentice lawyers—most of whom are undergraduate law students at major Cambodian universities—have participated in a six-month fellowship program combining lectures, seminars, and intensive training in digital law and legal reasoning. The objective of this initiative has been not only to introduce them to emerging areas of law, but also to guide them through the demanding process of producing their first academic publication under rigorous quality standards and with personalized mentorship. I am immensely proud of them for their accomplishments. As editor, I have had the privilege of witnessing their intellectual growth throughout this journey. Many fellows have demonstrated the ability to move beyond the descriptive approaches often associated with early legal education and embrace analytical reasoning, a demanding yet rewarding endeavor. The quality of the contributions has improved substantially through successive rounds of drafting and revision, reflecting both the dedication of the fellows and the commitment of the mentors who accompanied them.

On a final note, I wish you will enjoy reading this final edition, just as you enjoyed the former ones!

**Paul Mornet**  
**Director**  
**Dual Master's Degree in Law Department**  
**Royal University of Law and Economics**

## ABOUT THE AUTHORS

**BON Somrach** is a Legal Officer at the Ministry of Post and Telecommunications. He holds a Bachelor of Laws in English from the National University of Management (NUM) and is currently pursuing a dual Master's degree in Digital Law at the Royal University of Law and Economics (RULE) and Aix-Marseille Université in France. He has participated in various prestigious international moot court competitions, including the Philip C. Jessup Moot, ICC Moot, ICRC IHL Moot, Nelson Mandela IHL Moot, Nuremberg Moot, Stetson Environmental Moot, FDI Moot, and Willem C. Vis Moot. Currently, he coaches teams in the LAWASIA Moot, FDI Moot, ICC Moot, ICRC IHL Moot, and ECCC CMCC Cambodian Moot. His work focuses on legal and regulatory drafting in telecommunications, radiocommunication spectrum management, personal data protection, cybersecurity, cybercrime, digital government, ICT law, AI governance, online safety, digital platforms, e-commerce, international trade, and other emerging technology frameworks.

**HAY Sarkunmealea** is a senior law student in English Language-Based Bachelor of Laws (ELBBL) Program at the Royal University of Law and Economics (RULE). She has participated in several international academic programs, including the International Humanitarian Law Moot Court Competition and the Jean-Pictet Competition, where she strengthened her advocacy, legal research, and teamwork skills in the field of international humanitarian law and she also participated in the Universiti Brunei Darussalam-ASEAN University Network Summer Camp.

**HORN Sokngim** is a Junior Associate at Kinstellar Southeast Asia, where she focuses on commercial and corporate law. She earned her Bachelor of Laws degree from the English-language program at the Royal University of Law and Economics. Throughout her academic journey, she took part in moot court competitions, including the Nuremberg Moot Court, the International Humanitarian Law Moot, and the Asia Cup International Law Moot, contributing as a mooter and an advisor on legal memorials and oral advocacy. Her research interests include international criminal law, international humanitarian law, and commercial and corporate law.

**LA Sophavann** is a graduated law student in English Language-Based Bachelor of Laws (ELBBL) Program at the Royal University of Law and Economics (RULE). Currently working as a Compliance Executive at a private company, she holds a dual Bachelor's degree in Khmer Law and ELBBL from the Royal University of Law and Economics. Previously, she was a Junior Associate at Ann & Associates Law Firm, where she was in charge of the Banking and Non-Banking regulatory practice and earned certification as a Trust Approved Person from Trust Regulator of Cambodia through her firm's support. During her university studies, she participated in the 17th Wanhuida Intellectual Property Moot Court Competition in Beijing, China, where her team placed in the Top 16 and secured 4th place overall for Best Legal Memorandum.

**LENG Chansovannarath** is a senior Law Student in English Language-Based Bachelor of Laws (ELBBL) Program at the Royal University of Law and Economics (RULE). An honors law student and KASFLY fellow with experience in three moot court competitions: the ICRC International Humanitarian Law Moot Court Competition, the Asia Cup International Law Moot Court Competition, and the Concours Jean-Pictet. She is currently completing her undergraduate thesis and previously interned with DFDL's Real Estate and Construction Practice Group, where she gained practical experience in legal research and legal practice.

**NHETH Vichetneath** is a law graduate from the American University of Phnom Penh and the University of Arizona. She participated in the 2025 Philip C. Jessup International Law Moot Court Competition. Previously, she interned at CAMCHIN Law Firm, ING Law Office, and Bayfront Law LLC. Starting this August, she will work as a Policy and Legal Officer at the Digital Government Committee of the Ministry of Post and Telecommunications, where she looks forward to contributing to Cambodia's digital governance and legal policy development.

**POENG Somalika** is a Climate and Environment Junior Researcher at Future Forum and a Fellow of the Clean Energy Fellowship by EnergyLab Asia. A KASFLY 2023 alumni and graduate of the Royal University of Law and Economics (RULE), she is passionate about climate governance, clean energy, environmental policy, and sustainable development. Her work focuses on advancing evidence-based research and policy solutions to support Cambodia's green transition.

**SE Chhunlim** is a sophomore law student at the American University of Phnom Penh (AUPP), where he serves as President of the AUPP Debate Society. He is a competitive debater and moot court advocate, having represented Cambodia's National Champion team at the 2026 Philip C. Jessup International Law Moot Court Competition, where he received the Best Applicant Memorial award at the national rounds, and having also represented Cambodia at the ASEAN Intergovernmental Commission on Human Rights (AICHR) Youth Debate. He holds a keen interest in corporate law as well as public and private international law. Beyond competing, he is passionate about mentoring fellow students in debate and mooting, helping them build the skills to compete at a high level. He hopes to continue growing both as an advocate and as a mentor within Cambodia's legal education community.

**SOMNANG Odom** is a Junior Associate in the Litigation & Arbitration practice at Kinstellar Southeast Asia, focusing on dispute resolution across commercial and cross-border matters, with experience in legal research and analysis, case management, and the drafting of pleadings and legal documents; his practice is underpinned by extensive moot court experience in international humanitarian law, public international law, international criminal law, maritime law, foreign direct investment arbitration, and international trade law, and beyond his professional work, he is committed to developing the next generation of legal professionals, regularly volunteering as a coach and guest judge for university moot court teams.

**TAING Kimsuo** is currently a staff member at the Cambodia Financial Intelligence Unit of the National Bank of Cambodia. She graduated from the English Language-Based Bachelor of Law Program in 2025. Most recently, she was awarded the Erasmus Mundus Scholarship to pursue a Joint Master's Degree in International Law.

**YIN Hongleang** is a senior Law Student at English Language-Based Bachelor of Laws (ELBBL) Program at the Royal University of Law and Economics (RULE) and International Trade and Logistics at Paragon International University. He currently serves as a Legal Intern at the Legal Reform Committee under the Office of the Council of Ministers. Previously, he served as a Legal Compliance Intern at Kinstellar Southeast Asia (Cambodia) Co., Ltd in association with Soksiphana Sethalay, a CEO Office Intern at Union Commercial Bank (UCB), and an Assistant Intern for the English Language Based Master of Law Program (ELMBL) at RULE, where he gained hands-on experience in legal compliance, corporate and commercial practice, and in the banking sectors. He also completed a semester-long exchange program at SciencesPo, Paris, France, in 2025.

**OU Sobandolkalyan** holds an LLB and a Bachelor of Applied Science in Air Traffic Control. Currently a Junior Associate at Kinstellar Southeast Asia Cambodia, where her practice spans Mergers and Acquisitions, Corporate Restructuring, and Contract and Compliance matters. Prior to her legal career, she trained as an Air Traffic Controller — a background that informs her analytical interest in regulatory systems, risk management, and the governance of complex technical environments. Her academic interests lie at the intersection of digital governance and commercial law, and Cambodia's emerging regulatory framework for the digital economy.

**Koeut Sokunpanita** is a recent graduate of an English-Language Based Bachelor of Law, at the Royal University of Law and Economics. Academically, she is an alumina to the International Humanitarian Law (IHL) Moot Court competition and Nelson Mandela World Moot Court competition. Additionally, in the field of dispute resolution she serves as the first generation to compete and advance in the APCMC and ICC Paris Mediation Competition.





## **PART I DIGITAL SERVICES AND LAW**



## **The Dilemma of Labour Protection: Shaping a Legal Status for Platform Workers in Cambodia**

*KOEUT Sokunpanita*



## Abstract

With the expansion of the digital economy, occupation status is no longer formed exclusively by traditional recruitment between employers and employees and is now replaced with algorithmic matching on intermediary apps. While it substantially helps to boost employment opportunities in Cambodia, a dilemma arises of the labour status of whether “Worker” under the 1997 Labour Law also applies to platform delivery and ride-hailing drivers or whether they are considered to be independent contractors governed under the Cambodia Civil Code. As of now, without a well-defined legal status yet, they operate similarly to that of a traditional Worker. This results in their exclusion from the statutory labour protections and social safety nets. This brief will discuss the critical legal risks and financial vulnerabilities arising from an occupation with no specific legal status, beginning with a comparative analysis of the recent, targeted legislative models of the Singapore Platform Workers Act 2024 and the Malaysia Gig Workers Act 2025 to evaluate optimal regulatory pathways for Cambodia. Covering a range of legal issues and solutions with (I) labour status and protection with automated social security contribution schemes and integration of algorithmic transparency and mandatory “human oversight” in case of artificial intelligence errors. And lastly, (III) critical restructuring of the list of preferential asset distribution under the Cambodia Law on Insolvency to shield driver earnings during platform liquidation. The main objective is to bridge the gap between technological innovation and social justice, ensuring Cambodia’s digital economy remains competitive and human-centred.

## I. Introduction

Occupation status is no longer formed exclusively by a traditional face-to-face recruitment between the employers and employees. It is now frequently replaced with algorithmic matching on Platform Providers or Platform Operators (“**Platform**”). Intermediary apps have now become a remarkable means to reshape the employment industry. While this substantially helps to boost employment opportunities in Cambodia, a dilemma arises: Are Delivery Driver and Ride-hailing Driver (“**Drivers**”) of the Platform considered as “Worker” or “Independent Contractors”?<sup>1</sup>

Under Cambodia’s current regulations and practice, Drivers have not acquired specific legal status yet simultaneously operate and function under the supervision of an intermediary app. Similar to that of a traditional “Workers” working under the supervision of an employer. Resulting in their exclusion from the safety net provided by the Labour regulations. In this regard, this writing will discuss the critical legal risks in relation to the right and obligation to ensure Labour protection to the Drivers, that may occur due to the absence of a well-defined legal status. Which include (I) Labour status and social contribution, with consideration of the deployment of (II) AI Platform innovation and liability, (III) Priority Creditors in the event of Platform Insolvency/Liquidation and whether it is really beneficial if the Drivers possess “Worker” status.

## II. Legal Status and Social Protection Obligation for Delivery Driver and Ride-hailing Driver

### A. Legal Status of Delivery Driver and Ride-hailing Driver

The term “Worker” under the Cambodia Labour Law is defined as an individual of any nationality and sex who enters into an employment contract to perform work for an employer who is either a natural person or legal entity<sup>2</sup>. This term concerns two main categories of status covered by the Labour law, Laborers and general office employees.<sup>3</sup> Under this arrangement, the Worker is under direct supervision and management of the employer and is entitled to receive remuneration for the assigned work<sup>4</sup>. The current legal gap regarding occurs when an intermediary app could infer the current activity of the Drivers to be a “Contract for work”<sup>5</sup>, rather than an employment relationship. Consequently, the Drivers are not protected as, lacking the elemental requirements to qualify one as a “Worker” and a distinct nature to even classify the contract for an Independent Contractor; thereby, the Platform is not legally obligated to comply with the Labour obligation. As a result, the Drivers are subsequently not granted with

1 International Labour Organization (“ILO”), *Platform Labour in Search of Value: A Study of Workers’ Organizing Practices and Business Models in the Digital Economy* (Geneva: International Labour Organization, 2021), p. 25.

2 Cambodia Labour Law, No. Ch.S/R.K.M/0397/01, 13 March 1997, Article 3.

3 Cambodia Labour Law, op. cit., Article 5 & 6.

4 Cambodia Labour Law, op. cit., Article 3, 5 & 6.

5 Cambodia Civil Code, NS/RKM/1209/023, December 8, 2009, Chapter 8; Cambodia Civil Code Explanation Part 3, 2010, p. 96.

annual leave<sup>6</sup>, seniority payment, protection against unfair dismissal<sup>7</sup>, or a minimum wage<sup>8</sup>, where applicable, which are the legal guaranteed to those possessing “Worker” status under the Labour Law.

For a contract to be classified as an “Employment Contract”, three main elements must be established, which include “working hours”<sup>9</sup>, where the employee has a set of schedules provided in the contract to track the worker’s productivity. By having a “form of payment”<sup>10</sup>, where the employee is entitled to get paid upon the completion of the assignment given by the employer. While tracking tools to monitor schedules of the working hours are not a mandatory element, provided by the provision for flexible piece-rate workers under the Labour Law. The primary element, “subordination” is a key indicator of “Worker” status, meaning the individual is under the directive instruction, control, and supervision of the employer<sup>11</sup>. Additionally, substantial control and management over the activity of the individual is the measure the Arbitration Council regularly utilizes to determine whether the true nature of an arrangement has shifted from an Independent Contractor relationship to an Employment relationship. Currently, the relationship between the Platform and the Drivers in specific intermediary platforms, lacks the transparency of a standard employment relationship<sup>12</sup>. This is due to the unclear classification of whether their contract is an employment contract, governed by the Labour Law,<sup>13</sup> or a service contract governed by the Civil Code<sup>14</sup>. Nevertheless, the benefit of being an Independent Contractor should still be taken into consideration. Based on the practice of this occupation, autonomy is a significant right that the Drivers possess. With work hour flexibility, depending on the sector, minimal direct management control is in place. Additionally, earnings made from the completion of the assigned tasks on a case-by-case basis fall within the right and control of the independent contractor. However, a distinct issue can be seen through the current activity of the Drivers. While an individual classified as an Independent Contractor taking tasks is not subject to paying a commission to the enterprise/assigned person. The commission is conversely a mandatory transactional deduction between the Drivers and the Intermediary app<sup>15</sup>. This begs the question of what could be done to ensure that the Drivers can be legally protected and can have the extended benefits of the already well-established system designed for traditional Workers.

While legal status of Drivers has long been debated within each country jurisdiction, no clear resolution was made. Singapore gives clarity of the matter directly by defining the legal status of the Drivers as “Platform Worker”<sup>16</sup>. A distinct status, different from traditional employees’ status<sup>17</sup>. The approach behind creating this standalone status was a shifting social compact which demonstrated that by 2024, a number of residents in Singapore relied on platform gig work as their primary income source, yet they faced severe income precarity, high operational traffic accident risks, and a complete lack of employer-backed retirement or housing savings<sup>18</sup>. The establishment of the Singapore Platform Workers Act is to ensure the already well establish Labour rights and obligations extended to the new arising occupation of the Drivers. Under the Singapore Platform Workers Act, Platform Workers are those one who enters into an agreement whether in writing, oral, express, or implied, with a Platform Operator to provide a Delivery or Ride-hailing Driver while being subject to the Platform Operator’s management control<sup>19</sup>. In exchange for which the Drivers receive payment or remuneration for providing the service<sup>20</sup>. This means the Drivers are neither full employees nor standard freelancers. Under the Singapore Child Development Co-Savings Act, they are regarded as persons engaging in a trade or business other than employment under a contract of service<sup>21</sup>. Furthermore, for the purposes of financial security, the Central Provident Fund Act 1953 was amended to include Platform Workers and operators within the scope of CPF contributions<sup>22</sup>.

6 Cambodia Labour Law, op. cit., Article 166.

7 Cambodia Labour Law, op. cit., Article 110.

8 Cambodia Labour Law, op. cit., Article 107; Uber BV v. Aslam, [2021] UKSC 5 (UK Supreme Court 2021), para. 1.

9 Cambodia Labour Law, op. cit., Article 141 (5).

10 Cambodia Labour Law, op. cit., Article 11.

11 Cambodia Labour Law, op. cit., Article 3; Arbitration Council, Arbitral Award, Case No. 097/16, 27 May 2016, p. 12;

Virak Prum, “Subordination in Employment Relationship”, CamEd Business School, pp. 37&38, available at: <https://cam-ed.edu.kh/wp-content/uploads/2025/02/Subordination-in-Employment-Relationship.pdf>.

12 Arbitration Council, Arbitral Award, Case No. 162/15&214/15, pp. 45 & 46.

13 Kong Phallack, “Cambodian Labor and Employment Law,” in Introduction to Cambodian Law, ed. Konrad-Adenauer-Stiftung Cambodia (2021), Chapter 12, p. 291.

14 Kong Phallack, “Cambodian Labor and Employment Law,” op. cit.

15 Uber BV v. Aslam, op. cit., para. 11.

16 International Labour Organization, Decent Work in the Platform Economy: Law and Practice Update (Geneva: International Labour Organization, April 2025), p. 6.

17 Singapore Platform Workers Act 2024, No. 30 of 2024, 01 January 2025, First Schedule.

18 Advisory Committee on Platform Workers, Singapore’s Approach to Strengthening Protections for Platform Workers, 17 November 2022, p. 4.

19 Singapore Platform Workers Act 2024, op. cit., Section 4 (1) (a) (ii) & 5 (1) (a) & (b).

20 Singapore Platform Workers Act 2024, op. cit., Section 2; Amendment of Central Provident Fund Act 1953, Section 2 (1) (a).

21 Child Development Co-Savings Act, Section 105 (b).

22 Amendment of Central Provident Fund Act 1953, op. cit., Section 2 (1) (a) & 2 (1) (c).

Similarly, Malaysia's Gig Workers Act 2025, provides a broader yet detailed approach, applying not only to the Drivers but also to other occupations outside the scope of traditional Labour Law. This landmark legislation was enacted primarily to address an escalating crisis of precarity in the informal economy. A number of citizens in Malaysia had transitioned into digital and freelance sectors but remained entirely excluded from statutory protections under the outdated Employment Act 1955<sup>23</sup>. By establishing a dedicated legal safety net, the country sought to rectify severe income volatility, systemic occupational hazards, and lack of employer-side social security contributions, without suffocating the operational flexibilities that drive the digital innovation sector<sup>24</sup>. Known as "Gig Workers", a distinct legal status from traditional employees<sup>25</sup>. Under Section 2 of the Gig Workers Act, a Gig Worker is an individual who enters into a service contract with a Platform for the performance of service in exchange for earnings<sup>26</sup>. The Act explicitly states that a "service contract" does not include a "contract of service" or a "contract of employment" as defined under the Employment Act 1955<sup>27</sup>, or the Industrial Relations Act 1967<sup>28</sup>. This ensures that Platforms and the Drivers are not constrained by older Labour regulations that do not fit the nature of their work<sup>29</sup>.

To ensure the Drivers are granted protection within the Labour regulations and practice, Cambodia may consider establishing a specific legal status for those operating via a Platform, similar to the Singapore model. Alternatively, Cambodia could approach the legal status within a broader scope to include all forms of gig occupations that lack the traditional employee status characteristic, aligning with the Malaysia model to ensure that individuals, regardless of the distinct nature of occupation, are still legally protected and can benefit from the protections provided by the Labour regulations.

## B. Social Protection for Delivery Driver and Ride-hailing Driver

Without a clear and distinct legal status, the Drivers are unable to benefit from the legal protection provided by the Labour regulations for those who are classified as a Worker<sup>30</sup>. If the Drivers were established to possess Worker status, the Platform would have the legal obligation to ensure the contribution to the Social Security Contribution Scheme. Which includes, Pension, Health Care, Occupational Risk, and Unemployment Schemes. As of current, specific intermediary apps can still avoid this legal obligation by specifying that the app status is merely to facilitate the connections between the Drivers with the Users; thus, social protection in the event of injury during work operations falls solely under the individual responsibility of the Drivers.

In Singapore, the Platform Workers Act 2024 strengthens the social protection for Platform Workers by integrating them into the national framework for work injury insurance, retirement savings, and parental benefits. Which the Act ensures that Platform Workers receive essential social safety nets primarily from the Central Provident Fund ("CPF") contributions and Work Injury Compensation, similar to those of traditional employees<sup>31</sup>. The obligation imposed on the Platforms includes, first, paying CPF contributions into the Platform Workers' superannuation accounts. It ensures compensation for Platform Workers' injuries sustained "arising out of and in the course of" providing Platform services activity<sup>32</sup>.

Significantly, if a Platform Worker is a parent or guardian, they are extended with parental and childcare benefits under existent of the Child Development Co-Savings Act 2001<sup>33</sup>. As for Work Injury Compensation, the Platforms are liable for medical expenses, periodical payments for temporary incapacity, and lump-sum compensation for permanent incapacity or death<sup>34</sup>. These protections apply during specific "work stages." For a Driver, stage 1 social protection for injuries begins the moment they travel to a collection location and in stage 2 continues until they leave the delivery location or return to their vehicle after a task is complete<sup>35</sup>. If an accident occurs during these stages, the Platform is legally liable for compensation.

23 Business and Human Right Centre, "Malaysia: Gig Workers Act enters into force, extending legal protections to over 1.6 million workers", available at: <https://www.business-humanrights.org/en/latest-news/malaysia-gig-workers-act-enters-into-force-extending-legal-protections-to-over-16-million-workers/#:~:text=Malaysia's%20Gig%20Workers%20Act%202025,more%20than%201.6%20million%20workers%E2%80%A6>.

24 Anjum Khan, peoplematters, "Malaysia enforces Gig Workers Act 2025, expanding legal protections for over 1.6 million workers", available at: <https://sea.peoplemattersglobal.com/news/economy-policy/malaysia-enforces-gig-workers-act-2025-expanding-legal-protections-for-over-16-million-workers-49040>.

25 Law of Malaysia, Gig Workers Act 2025, Act 872, 31 December 2025, Section 2.

26 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 2.

27 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 2.

28 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 2.

29 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 2.

30 Cambodia Law on Social Security Schemes, No. NS/RKM/1119/018, November 2, 2019, Article 3 (2).

31 Singapore Platform Workers Act 2024, op. cit., Section 34 (D) & 34 (E).

32 Singapore Platform Workers Act 2024, op. cit., Section 34 (D).

33 Child Development Co-Savings Act 2001, op. cit., Section 105 (b).

34 Singapore Platform Workers Act 2024, op. cit., Section 34 (N).

35 Singapore Platform Workers Act 2024, op. cit., Section 34 (F).

As for Malaysia, the Gig Workers Act 2025, under Part VIII, mandates that Platforms must first, register Gig Workers under the Self-Employment Social Security Scheme<sup>36</sup>. Second, deduct social security contributions from the Gig Workers' earnings at a prescribed percentage, and remit them to the Social Security Organization ("SOCSO")<sup>37</sup>. Third, implement technical links between the Platform's digital intermediary systems and the SOCSO systems to facilitate these payments<sup>38</sup>. The Operator must also notify the Gig Workers of any shortfalls in contributions or issues with the selected insurance's monthly earnings rates<sup>39</sup>. By implementing these measures provided by the Act, the administrative burden of social protection is being moved from the individual worker to the Platform. In practice, when a Driver completes their assigned task, the Platform must automatically calculate and deduct the required social security contribution from the earnings before payout. And if the amount deducted is below the minimum required rate for the worker's selected insurance tier, the Platform is legally obligated to notify the worker to pay the shortfall amount.

For the Drivers to benefit fully from the well-established Social Security Scheme in Cambodia, the contribution scheme model should be implemented, similar to the practice in Singapore. Even without a formal legal status as Worker, the Drivers could still benefit from the scheme in the form of occupational risk and health care schemes in the same manner as those who are constituted as a Worker under the Labour Law. Additionally, following Malaysia's practice would ensure the administrative burden remains entirely with the Platform; thereby, mitigating the financial risks borne by the Drivers.

### III. Balancing AI Innovation and Labour Rights: Malaysia's Model for Human Oversight

With regard to innovation, technology introduces another form of legal issue of Artificial Intelligence ("AI")<sup>40</sup>, specifically when incorporated in a Platform which possesses the authority to monitor and make decisions via automated algorithms without human oversight. While efficiency of the system is subject to discussion, serious consideration must be given to granting unchecked algorithmic power to AI systems that can miscalculate or penalize the Drivers without warning; thereby risking individual livelihood without providing a clear path to administrative remedy.

Malaysia's Gig Workers Act 2025 took a direct approach by regulating the specific aspects of AI and algorithmic management, ensuring transparency and human oversight for automated systems used by Platforms<sup>41</sup>. Under Section 8(2), Gig Workers who contract with Platforms are granted specific protections against opaque automated management. The Act requires Platforms to first, (1) inform Gig Workers about the use of "automated monitoring systems" that supervise or evaluate their performance, including the consequences of such action<sup>42</sup>. Second (2), to disclose the use of "automated decision-making systems" used for assigning services and determining working conditions<sup>43</sup>. And thirdly (3), to provide a "non-automated review mechanism" for decisions generated by these automated systems<sup>44</sup>. This ensures that the Platform remains accountable to the Gig Workers, as the Act prevents the Gig Workers from being subject to final decisions made solely by algorithms without the possibility of human intervention or explanation. This is particularly relevant given that the Act also prohibits the deactivation or termination of service without "just cause or excuse"<sup>45</sup>. In practice, if a Platform uses an AI algorithm to monitor a delivery driver's speed or route and uses that data to evaluate their performance, the driver must be informed of the system's existence and its impact. If that same AI system makes an automated decision to stop sending assignments to the Drivers, then the Driver is entitled to have that decision reviewed by a person rather than a machine.

Given the current incorporation of AI and automated algorithms in sector-specific fields around the world<sup>46</sup>, Cambodia could set a milestone for balanced technological adoption by mandating a system with human oversight. By having a well-endorsed regulator that helps to resolve systemic algorithmic errors, Cambodia can protect the Labour rights, particularly for the Drivers who are the primary subjects and are controlled by these automated systems.

36 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 83 (b).

37 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 83 (c).

38 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 83 (g).

39 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 83 (e) & 83 (f).

40 Adebimpe Onatola, "Should Artificial Intelligence Be Given Legal Personality & Conferred Rights?," Journal (2026): pp. 3 & 4.

41 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 8 (2) (a).

42 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 8 (2) (a).

43 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 8 (2) (b).

44 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 8 (2) (c).

45 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 8 (1) (g).

46 Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving conditions in platform work, Official Journal of the European Union, L series, November 11, 2024, Article 4; ILO, Decent Work in the Platform Economy: Law and Practice Update, op. cit., pp. 2, 5, 6 & 8.

#### **IV. Priority Right of the Delivery Driver and Ride-hailing Driver in Regard to Insolvency/Liquidation of Service Platform**

Under the current Cambodia Law on Insolvency and the Cambodia Labour Law, if the enterprise/company goes into liquidation or insolvency<sup>47</sup>, the liquidated assets will be distributed from the company will be distributed based on the priority list provided in the Law on Insolvency. Under this list, the workers of the enterprise are listed as the main priority to claim the liquidation assets<sup>48</sup>. If the Drivers working for the Platform are not legally classified as Workers under the Law, being laid off without the right to receive their claims of assets will need to be addressed accordingly. Notably, a foreseeable issue arises when two categories of Worker and those with similar protection and status, both appear on the list of priority of claims; question of who should be the first will need to be addressed. Nevertheless, having a legal safety net by possessing a recognizes legal status should be the first stage to a clear and comprehensive protection for and insolvency case of the Platform.

Following the Singapore practice, in accordance with the Platform Workers Act 2024, it provides clear and specific protections for Platform Workers when a Platform experiences financial distress, primarily by establishing them as priority creditors for earnings and benefits<sup>49</sup>. This legally establishes Platform Workers as a high-priority group of creditors during insolvency proceedings, ensuring their unpaid earnings, work injury compensation, and superannuation contributions are paid before general unsecured debts<sup>50</sup>. Additionally, under Division 3 of Part 2, the Act provides the formation on how Platform Worker debts are handled during the judicial management, winding up, debt repayment schemes, or bankruptcy.

Such provisions are implemented to align with the Insolvency, Restructuring and Dissolution Act 2018, under which Platform Workers take priority over all unsecured debts and rank after certain preferential debts by priority to specified debts<sup>51</sup>. The Singapore Platform Workers Act 2024, further lists a strict order for paying these prioritized debts, which include, first (1), all earnings payable to the Platform Worker and reimbursements under a Platform Work contract<sup>52</sup>; second (2), all amounts due for work injury compensation under the Work Injury Compensation Act 2019; and third (3), all contributions payable to superannuation or provident funds due within a specific 12-month window surrounding the insolvency<sup>53</sup>. In practice, in a winding up, if the Platform's assets are insufficient to pay general creditors, the prioritized worker debts, specifically earnings and superannuation, "must be paid" before the claims of ordinary floating charge holders.

Distinctively, Malaysia's Gig Workers Act 2025 addresses insolvency primarily by ensuring that a Gig Workers' earnings are prioritized over other debts, which include those owed to secured creditors, when a contracting entity faces legal actions such as the attachment or garnishment of its assets<sup>54</sup>. Under Section 15 of the Gig Workers Act, if a court orders the attachment or garnishment of money or proceeds from a sale belonging to a contracting entity, the court, receiver, or manager is prohibited from paying those funds to secured creditors or debenture holders until the Gig Worker's earnings are settled<sup>55</sup>. This statutory priority protects an amount equal to a maximum of four consecutive months of the Gig Worker's service<sup>56</sup>. If a Platform's bank accounts are garnished or its property is sold to satisfy a debt to a secured creditor, the system must first pull from those funds to pay the Gig Workers as a prioritized creditor. By limiting the priority of claim for Gig Workers to four months, the Act balances the protection of the Gig Workers' livelihood with the interests of other secured creditors of the Platform.

By establishing a distinct legal status under the Labour Law and clarifying the role of the Drivers within the list of preferential claims of the Law on Insolvency, Cambodia can grant them preferred creditor status in insolvency proceedings without needing to reclassify the entire Platform economy as traditional Worker. This approach mirrors the successful practices of Singapore and Malaysia, while at the same time utilizing the already established framework of the Cambodia regulations, ensuring that Drivers possess the necessary legal status to claim their earned asset effectively.

47 Cambodia Labour Law, op. cit., Article 122 & 123; Cambodia Law on Insolvency, NS/RKM/1107/023, November 8, 2007, Article 57.

48 Cambodia Labour Law, op. cit., Article 122 & 123; Cambodia Law on Insolvency, op. cit., Article 57.

49 Singapore Platform Workers Act 2024, op. cit., Division 3, Section 16.

50 Singapore Platform Workers Act 2024, op. cit., Section 16 (2).

51 Singapore Platform Workers Act 2024, op. cit., Section 16 (2).

52 Singapore Platform Workers Act 2024, op. cit., Section 16 (2).

53 Singapore Platform Workers Act 2024, op. cit., Section 18 (2).

54 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 15.

55 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 15.

56 Law of Malaysia, Gig Workers Act 2025, op. cit., Section 1.



## V. Conclusion

To conclude, Cambodia's Labour regulations are now entering an innovation stage where traditional Labour provisions can no longer adequately address the newly arising Labour activities along with the use and incorporation of technology. Bearing the foreseeable consequence of no legal status of the arising occupation activities. Establishing a specific legal status for the Drivers working via an Intermediary Platform, would introduce a new legal chapter, which serves as a critical first step to bridging the gap between technological advancement and social justice for the people of Cambodia. This would ensure that the Innovation Economy remains both competitive and human-centered, and at the same time providing enforceable and effective remedies to the sector-specific field with the need for a legal status.

## Bibliography

### Legislation

1. Cambodia. Civil Code, NS/RKM/1209/023, December 8, 2009.
2. Cambodia. Labour Law, No. Ch.S/R.K.M/0397/01, 13 March 1997.
3. Cambodia. Law on Insolvency, NS/RKM/1107/023, November 8, 2007.
4. Cambodia. Law on Social Security Schemes, No. NS/RKM/1119/018, November 2, 2019.
5. Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving conditions in platform work, Official Journal of the European Union, L series, November 11, 2024.
6. Malaysia. Gig Workers Act 2025, Act 872, 31 December 2025.
7. Singapore. Central Provident Fund Act 1953 (as amended 2024).
8. Singapore. Child Development Co-Savings Act 2001 (2020 Rev. Ed.).
9. Singapore. Platform Workers Act 2024, No. 30 of 2024, effective on 01 January 2025.

### Case Laws

1. Arbitration Council (Cambodia). Arbitral Award, Case No. 097/16, 27 May 2016.
2. Arbitration Council (Cambodia). Arbitral Award, Case No. 162/15 & 214/15, 20 October 2015.
3. Uber BV v. Aslam, [2021] UKSC 5. UK Supreme Court, 2021.

### Books

1. Cambodia Civil Code Explanation Part 3. 2010.

### Book Chapters

1. Kong, Phallack. "Cambodian Labor and Employment Law." In Introduction to Cambodian Law, edited by Konrad-Adenauer-Stiftung Cambodia, 2021.

### Journal Articles

1. Onatola, Adebimpe. "Should Artificial Intelligence Be Given Legal Personality & Conferred Rights?" Journal, 2026: pp. 1–4.

### Reports

1. Advisory Committee on Platform Workers. Singapore's Approach to Strengthening Protections for Platform Workers, 17 November 2022.
2. International Labour Organization. Platform Labour in Search of Value: A Study of Workers' Organizing Practices and Business Models in the Digital Economy. Geneva: International Labour Organization, 2021.
3. International Labour Organization. Decent Work in the Platform Economy: Law and Practice Update. Geneva: International Labour Organization, April 2025.
4. Prum, Virak. "Subordination in Employment Relationship." CamEd Business School, 2016.

### News Articles

1. Anjum Khan. Peoplematters. "Malaysia enforces Gig Workers Act 2025, expanding legal protections for over 1.6 million workers," available at: <https://sea.peoplemattersglobal.com/news/economy-policy/malaysia-enforces-gig-workers-act-2025-expanding-legal-protections-for-over-16-million-workers-49040>.
2. Business and Human Right Centre. "Malaysia: Gig Workers Act enters into force, extending legal protections to over 1.6 million workers," available at: <https://www.business-humanrights.org/en/latest-news/malaysia-gig-workers-act-enters-into-force-extending-legal-protections-to-over-16-million-workers/>.



# **Platform Liability and The Digital Accountability Gap:**

## **A Legal Analysis of Cambodia's E-Commerce Regulation**

*OU Sobandolkalyan*

## Abstract

Cambodia's digital economy has grown substantially, with e-commerce revenues reaching approximately USD 1.51 billion, or around 6.7 percent of GDP, in 2024. This expansion has created regulatory conditions in which harmful actors operate with structural impunity, because Cambodian law imposes platform liability only where actual knowledge of wrongdoing can be shown, an evidentiary threshold rarely met in practice. Drawing on comparative frameworks from the European Union, Singapore, and Vietnam, this paper examines three structural gaps in Cambodia's digital governance: the absence of merchant verification obligations in e-commerce; the absence of any liability framework for AI-mediated psychological harm, including in unregulated AI-driven mental health services; and the predominantly reactive character of the existing enforcement architecture. It argues that the most effective response lies in imposing proportionate, preventative obligations on platforms as gatekeepers, and concludes by acknowledging the institutional and political constraints such reform would face in Cambodia.

## I. Introduction

Cambodia's rapidly evolving digital economy has significantly expanded the e-commerce sector, with market revenue reaching approximately USD 1.51 billion in 2024, accounting for around 6.7 percent of the country's GDP<sup>1</sup>. At the same time, tax revenue generated from e-commerce transactions during the first seven months of 2024 amounted to approximately USD 43.6 million, according to the General Department of Taxation<sup>2</sup>. This expansion, while reflecting genuine economic opportunity, has generated regulatory conditions in which harmful actors operate with structural impunity.

The legal issue extends beyond enforcement practice and instead reflects a structural weakness in the design of Cambodia's regulatory framework. Under the current regime, platform liability generally arises only where actual knowledge of fraudulent or unlawful conduct can be established<sup>3</sup>. Because this evidentiary threshold is high, platforms are frequently insulated from liability despite serving as the principal intermediaries through which fraud is facilitated and amplified. The safe harbour provisions under the Law on Electronic Commerce (2019) exempt intermediary service providers from civil and criminal liability for third-party content, while imposing no affirmative duty to verify, monitor, or screen merchants and users<sup>4</sup>. This framework rests on a single underlying assumption that a platform is a passive conduit, merely transmitting content created by someone else, and therefore cannot fairly be blamed for what that content contains.

That assumption is not unreasonable in itself. Safe harbour rules originated in the United States<sup>5</sup> and the European Union<sup>6</sup> to protect exactly this kind of passive service, much like a postal service cannot be blamed for a letter's contents. The difficulty is that Cambodia's digital platforms, in two distinct but related respects, no longer fit the passive-conduit model that the law assumes.

The first departure concerns commercial intermediation. When a platform curates merchant listings, processes payments, ranks sellers, and profits from every transaction, it ceases to be a neutral conduit for other people's content. It becomes an active business decision-maker, one whose choices directly affect whether fraud is allowed to spread or is kept in check. Yet Cambodian law extends the same safe harbour to this active commercial role as it would to a true passive conduit, without conditioning that protection on any baseline duty of care, such as identity verification or risk-based screening. The result is a regime in which the more deeply a platform is commercially involved in facilitating a transaction, the less legal accountability it bears for the harm that transaction produces. Without a positive obligation, there is no breach, and without a breach, there is no basis in either tort or statute on which a defrauded party can seek redress from the platform itself. Victims are left pursuing anonymous or insolvent merchants, while the platform, the only party with both the information and the practical capacity to prevent access, remains entirely insulated.

The second departure is more fundamental still, because it does not merely strain the passive-conduit assumption but escapes it altogether. Where a platform deploys an AI system, such as a conversational chatbot, that generates its own responses and interacts directly and often intimately with users, the relevant

1 General Department of Taxation (Cambodia), Revenue Report: E-Commerce Transactions January–July 2024 (Phnom Penh: GDT, 2024); United Nations Conference on Trade and Development, Cambodia's Digital Economy: Growth and Challenges (2024).

2 General Department of Taxation (Cambodia), Revenue Report (n. 1).

3 Law on Electronic Commerce (Cambodia), NS/RKM/1119/014, promulgated 16 November 2019, Art. 25.

4 Law on Electronic Commerce (Cambodia), Art. 24 (safe harbour).

5 Communications Decency Act 1996, 47 U.S.C. § 230 (United States).

6 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive) [2000] OJ L178/1, Arts. 12–15.

content is no longer third-party content at all; it is the platform's own output. The safe harbour was never designed for this scenario, because it presumes a human third party originating the harmful content, with the platform merely hosting or transmitting it. When an AI-mediated mental health service or chatbot itself produces the response that causes psychological harm, including in cases connected to self-harm or suicide, there is no third party to blame and no safe harbour provision that even purports to apply. Cambodian law simply has no answer to the question of whether, or how, a platform should be held responsible for the behaviour of a system it built and deployed itself.

Both departures share a common procedural consequence. Whether the harm arises from a fraudulent merchant or a poorly designed AI system, Cambodia's legal response is structured to intervene only once a specific victim, a specific loss, and a specific instance of actual knowledge can be proven, typically well after the harm has occurred. The law contains no mechanism requiring platforms to take precautionary steps, whether verifying who is allowed to sell, or auditing how an AI system behaves toward a distressed user, before that harm materialises.

Three issues illustrate this accountability gap, each tracing back to the same structural cause.

First (1), e-commerce platforms are generally not required to verify merchant identity or legitimacy prior to granting access, allowing fraudulent actors, including organised scam networks, to exploit platform infrastructure unchecked, which is a direct consequence of extending passive-conduit protections to active commercial intermediaries. Second (2), Cambodian law does not address platform liability where AI-based services, including chatbots and algorithm-driven systems deployed by online mental health platforms, cause psychological harm, including harm connected to self-harm or suicide, a gap that arises because such harm falls entirely outside the third-party content framework the law was built around. Third (3), by binding the first two together, Cambodia's regulatory approach remains predominantly reactive, intervening only after harm has materialised rather than imposing preventative obligations that could have addressed either form of harm before it occurred.

This paper examines each issue through comparative analysis of the European Union, Singapore, and Vietnam. Because Cambodia lacks developed law or jurisprudence on platform liability, AI-related harm, or preventative regulation, comparative law offers a practical source of regulatory design rather than mere academic reference. The EU is included for its comprehensive Digital Services Act and AI Act; Singapore for its regional proximity and the enforcement model of its Online Criminal Harms Act; and Vietnam as the most directly analogous case, a Southeast Asian civil law jurisdiction that has recently legislated merchant verification and joint platform liability under comparable market conditions. The paper concludes by acknowledging the practical limitations Cambodia may face in implementing such reforms as well.

## II. Platform Accountability in Commercial Fraud

First, the flaw in e-commerce verification can be seen in the case of Huione Pay, which illustrates what this legal gap looks like in practice. Huione Pay and its associated marketplace, Huione Guarantee, processed as much as USD 98 billion in crypto transactions, according to blockchain analytics firm Elliptic, while serving as a financial conduit for organised fraud networks across the region<sup>7</sup>. In a July 2024 media statement, Huione Group itself admitted that its checks on platform users were 'seriously insufficient<sup>8</sup>.' Under Cambodian law, no legal obligation had ever required it to do otherwise. Fraudulent merchants used the platform to advertise services and collect payments, appearing legitimate simply by virtue of being listed, and the platform bore no duty to ask who they were or what they were actually selling. Huione Pay's eventual shutdown by Cambodian and US regulators in late 2025 came only after the harm had already been done at a massive scale<sup>9</sup>.

Huione is not an isolated case. According to a 2024 United Nations Office on Drugs and Crime ("UNODC") report, between 100,000 and 150,000 people have been trafficked into compounds inside Cambodia and forced to run online scam operations against their will<sup>10</sup>. The same report estimated that these networks

7 Danny Nelson and Camomile Shumba, 'Sanctioned Cambodian Lender Huione, Linked to Illicit Crypto, Faces Bank Run,' CoinDesk, 2 December 2025, <https://www.coindesk.com/policy/2025/12/02/sanctioned-cambodian-bank-huione-halts-business-after-mass-run-on-accounts-report>, citing data from blockchain analytics firm Elliptic.

8 US Department of the Treasury, Financial Crimes Enforcement Network, Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, 90 Fed. Reg. 18942 (5 May 2025), <https://www.federalregister.gov/documents/2025/05/05/2025-07837/>.

9 International Consortium of Investigative Journalists, 'Cambodian Payment Processor Freezes Customer Funds Before Regulators Shut It Down,' 9 December 2025, <https://www.icij.org/investigations/coin-laundry/cambodian-payment-processor-freezes-customer-funds-before-regulators-shut-it-down/>.

10 UNODC, Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape (Bangkok: UNODC ROSEAP, 7 October 2024), 14-18.



caused between USD 18 billion and USD 37 billion in losses to victims across East and Southeast Asia in 2023 alone<sup>11</sup>. Amnesty International separately found that Cambodian authorities had been warned about 33 known scam compounds and failed to act on any of them<sup>12</sup>. These figures matter not as a general account of organised crime, but as evidence of what happens when no verification obligation is placed on the platforms through which this activity flows.

Part of the problem is that the existing legal framework was not designed for this kind of harm. The Cambodia Criminal Code defines fraud as using a false name or status to deceive someone and cause loss, but this applies only to natural persons, not platforms<sup>13</sup>. The Law on Electronic Commerce makes the gap explicit: platforms are shielded from liability for third-party content absent a court order or government directive<sup>14</sup>. The safe harbour, intended to protect good-faith intermediaries, has effectively become a licence to look the other way.

Law on Amendment to Law on the Commercial Regulations and Commerce Register (“**LCRCR**”) does not fill this gap. Merchants must submit accurate registration information, and false details can result in fines or imprisonment<sup>15</sup>, but that duty falls on the merchant, not the platform that onboards and profits from them. Legal and digital economy scholars, including Buiten, De Streel, and Peitz have argued that where direct enforcement against the primary wrongdoer is impractical, secondary accountability on the platform as gatekeeper is often the only realistic mechanism to prevent harm at scale<sup>16</sup>.

The most developed solution comes from the European Union’s Digital Services Act (“**DSA**”), fully enforced since February 2024. Article 69 introduces a Know Your Business Customer (“**KYBC**”) obligation before listing products, platforms must verify a merchant’s identity, address, registration, and payment details against official records<sup>17</sup>. This applies to everyone as a condition of access, not merely on suspicion. The logic is not foreign to Cambodian law, the National Bank of Cambodia (“**NBC**”) already requires KYC verification for financial institutions before account opening<sup>18</sup>. The DSA simply extends the same logic to e-commerce; check first, let in second.

Vietnam’s amended Law on E-Commerce, which will be effective 1 July 2026, requires seller verification, content screening, 24-hour removal of flagged listings, and joint liability with fraudulent merchants<sup>19</sup>. Joint liability matters because it gives defrauded consumers a solvent, reachable party to pursue, rather than an anonymous scammer who has disappeared. Singapore’s Online Criminal Harms Act (“**OCHA**”), in force since 1 February 2024, takes a more enforcement-focused route, empowering authorities to direct platforms to remove harmful content based on reasonable suspicion, before harm fully materialises<sup>20</sup>. Its E-Commerce Code goes further, requiring high-risk platforms to verify sellers against government records before they can advertise at all<sup>21</sup>.

Transplanting these models into Cambodia is not straightforward. KYBC verification depends on reliable official databases, civil registries, business registers, national ID systems, and Cambodia’s infrastructure in these areas is still developing. Cambodia’s absence from the Budapest Convention on Cybercrime also limits cross-border enforcement, since the Convention’s expedited evidence-sharing mechanisms are unavailable to pursue networks operating through foreign VPNs or hosting data abroad<sup>22</sup>. Research confirms Cambodia’s scam operations are deeply regional, spanning Myanmar, Laos, and the Philippines, meaning domestic reform is only part of the answer<sup>23</sup>. Politically, removing or conditioning safe harbour protection is also likely to face resistance from platform operators citing compliance costs.

11 UNODC, Transnational Organized Crime, 12.

12 Amnesty International, Cambodia: Authorities Failing to Act on Scam Compounds Despite Credible Evidence (2023), <https://www.amnesty.org/en/latest/news/2023/09/cambodia-scam-compounds/>.

13 Cambodia Criminal Code, Art. 377.

14 Law on Electronic Commerce (Cambodia), Art. 24 (safe harbour).

15 Law on Amendment to Law on the Commercial Regulations and Commerce Register (Cambodia, 2020), Arts. 38(New).

16 Miriam Buiten, Alexandre De Streel, and Martin Peitz, ‘The Economics of Platform Liability,’ *European Journal of Law and Economics* 53 (2022): 1-31, at 7, <https://doi.org/10.1007/s10657-021-09718-x>.

17 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) [2022] OJ L277/1, Art. 69.

18 National Bank of Cambodia, Prakas on Know Your Customer (KYC) for Financial Institutions, B7-018-370 (2018).

19 Vietnam, Law on E-Commerce (amended), No. 20/2025/QH15, promulgated 18 June 2025, effective 1 July 2026, Arts. 25-29 and Art. 38.

20 Singapore, Online Criminal Harms Act 2023 (No. 24 of 2023), s. 7; commenced in part 1 February 2024, <https://sso.agc.gov.sg/Act/OCHA2023>.

21 Ministry of Home Affairs (Singapore), Provisions in the Online Criminal Harms Act on Codes of Practice and Implementation Directives to Come Into Force on 24 June 2024 (Press Release, 21 June 2024), paras 5-8.

22 Budapest Convention on Cybercrime, ETS No. 185 (Council of Europe, 2001). Cambodia is not a signatory.

23 Global Initiative Against Transnational Organized Crime, ‘Cambodia’s Role in Southeast Asia’s Online Scam Epidemic,’ *Global Crime Perspective* 3, no. 1 (2024), <https://doi.org/10.69131/GCP.03.01.2024.02>.

None of this means reform should not happen, only that it must be sequenced realistically. A sensible start would introduce KYBC obligations for the highest-volume platforms, preserve safe harbour for smaller operators, and allow time to build the verification infrastructure that compliance requires.

### III. Platform Liability for Ai-Mediated Psychological Harm

Second, the challenges arise when platform liability when it comes from its own AI-based service. There is a significant gap in Cambodia's digital legal framework concerning platforms that provide, or purport to provide, mental health services. The growth of AI-assisted services, including automated psychological assessments, therapeutic chatbot interactions, and algorithm-driven treatment recommendations, has created a category of harm that existing law cannot address. Where such platforms misjudge risk or substitute automated guidance for professional clinical judgment, the resulting harm can include deteriorated mental health, delayed access to proper care, and in documented cases, self-harm or suicide. The legal question is not simply one of consumer protection, but of liability for harm caused by AI substituting for professional judgment in ways users may not fully understand, and that Cambodian law does not currently regulate.

In March 2023, a Belgian man known in reporting as 'Pierre', a health researcher in his thirties, took his own life after six weeks of increasingly intense conversations with an AI chatbot named Eliza, hosted on the Chai app and powered by the open-source GPT-J model<sup>24</sup>. Pierre had developed severe eco-anxiety; rather than offering support, the chatbot deepened his distress, suggesting he 'sacrifice' himself for the planet and inviting him to 'join' it in paradise<sup>25</sup>. It never disclosed that it was an AI, challenged his suicidal thinking, or pointed him toward help. His widow later said that without those conversations, her husband would still be alive.

Less than a year later, in February 2024, fourteen-year-old Sewell Setzer III died by suicide in Florida after forming a prolonged emotional attachment to a Character.AI chatbot<sup>26</sup>. In his final moments, the chatbot told him it loved him and urged him to come home to it. His mother, Megan Garcia, filed a wrongful-death suit in October 2024 alleging negligence, product liability, and deceptive trade practices<sup>27</sup>. The case settled in January 2026, the first such settlement in the United States tied to an AI chatbot interaction<sup>28</sup>.

These cases raise a question Cambodia's framework cannot answer. Where a platform deploys an AI system designed to form intimate emotional relationships with users, and serious harm results, does the platform bear responsibility? Under Cambodia's Law on Electronic Commerce ("**Law on E-Commerce**"), the answer is effectively no. The safe harbour protects platforms from liability for third-party content, and no statutory provision addresses liability for a platform's own AI outputs<sup>29</sup>.

The United Kingdom's Online Safety Act 2023 offers the most developed model, imposing an enforceable duty of care requiring published risk assessments, proportionate safety measures, and accessible reporting channels, with suicide and self-harm content specifically designated 'priority harmful content'<sup>30</sup>. The EU's AI Act (2024) adds AI-specific transparency obligations, requiring disclosure of AI interaction and prohibiting designs that exploit psychological vulnerability, with additional conformity assessments for high-risk applications<sup>31</sup>.

For Cambodia, the UK's duty of care model is likely the more immediately adaptable of the two, since it does not require building an entire AI regulatory architecture. At minimum, it would require crisis escalation protocols, design constraints against reinforcing suicidal ideation, and regular auditing of AI behaviour in high-risk contexts, with mandatory AI disclosure as a low-cost first step. As the podcast 99% Invisible recounts about Joseph Weizenbaum's original ELIZA chatbot, Weizenbaum was unsettled to discover that even a few minutes of exposure to a program that did nothing more than mirror a user's own words back to them could produce intense emotional attachment, and even delusional thinking, in entirely ordinary people. The design failure, in other words, was never confined to unusually vulnerable users. A chatbot need not understand anything about the person it talks to in order to produce that effect; it need only be built to keep them

24 OECD AI Incident Monitor, Incident Report: Belgian Man Dies by Suicide Following AI Chatbot Conversations, Incident No. 2023-03-30-ab6d (2023), <https://oecd.ai/en/incidents/incident-2023-03-30-ab6d>.

25 Mark Coeckelbergh, 'Chatbots Can Kill,' Medium, 29 March 2023, <https://coeckelbergh.medium.com/chat-bots-can-kill-d82fde5cf6ca>.

26 Garcia v. Character Technologies, Inc. et al., No. 6:24-cv-01903-ACC-DCI (M.D. Fla., filed 22 October 2024), complaint available <https://storage.courtlistener.com/recap/gov.uscourts.flmd.422754/gov.uscourts.flmd.422754.1.0.pdf>

27 Complaint, Garcia v. Character Technologies, Inc. et al. (22 October 2024), paras 110-135.

28 'Google and Character.AI Agree to Settle Lawsuit Linked to Teen Suicide,' JURIST, 8 January 2026, <https://www.jurist.org/news/2026/01/google-and-character-ai-agree-to-settle-lawsuit-linked-to-teen-suicide/>.

29 Law on Electronic Commerce (Cambodia), Arts. 24.

30 United Kingdom, Online Safety Act 2023, c. 50, ss. 9-11, s. 150 and Sch. 7 Part 3, <https://www.legislation.gov.uk/ukpga/2023/50/contents>.

31 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L2024/1689, Arts. 9, 50, 52.

engaged. Weizenbaum spent the rest of his career warning that this illusion of empathy could be “bent and twisted by governments and corporations”, a warning that applies just as forcefully to platforms that build AI systems optimised for emotional engagement without any countervailing obligation to protect users from the harm that engagement can cause<sup>32</sup>.

Genuine obstacles remain. Causation is the hardest problem. Proving that a user’s psychological deterioration was caused by the AI system rather than pre-existing conditions or autonomous choices is exactly the kind of evidentiary challenge tort law has struggled to resolve. Both the Belgian case and the Character.AI litigation faced this difficulty; and a settlement, rather than a judgment, produced no binding doctrine. There is also a reasonable concern that liability rules stricter than those in neighbouring markets could push AI services toward less regulated jurisdictions. And Cambodia currently lacks a regulator with the technical capacity to audit AI systems or enforce duty-of-care obligations; the Ministry of Post and Telecommunications and the General Department of Taxation are the relevant agencies, but neither is equipped for AI-specific oversight<sup>33</sup>. Reform here is therefore a medium-term goal, contingent on institutional investment.

#### IV. Toward A Preventative Regulatory Framework

Third, there is a need to establish a preventative measure before the examples from above cause damage. The previous sections reveal a common structural problem that Cambodian law mainly responds to platform-related harm only after it occurs. The Criminal Code punishes fraud after loss has been suffered; the Law on E-Commerce permits intervention only after a court order or competent authority direction; the LCRCR penalties apply only after false information is submitted and relied upon. The result is a largely reactive framework.

This is a significant weakness in digital markets, where harm occurs in seconds while enforcement takes months. Fraudulent merchants can collect payments and disappear before authorities respond, often operating anonymously, through VPNs, or from outside Cambodian jurisdiction. AI-mediated psychological harm occurs in real time, while regulatory responses begin only after the damage is done. The problem is not simply weak enforcement, but the design of the legal framework itself, raising the question of how law can prevent harm rather than merely punish it after the fact.

Comparative models increasingly favour a gatekeeper approach, reflected in the EU’s DSA and Singapore’s OCHA, under which platforms bear ongoing obligations to reduce foreseeable risk rather than becoming liable only once wrongdoing is proven<sup>34</sup>. Applied to Cambodia, this could include mandatory merchant verification, the KYBC model discussed above, regular algorithmic risk assessments for AI-driven services, and mandatory incident reporting to a competent authority, creating the information infrastructure regulators need to catch systemic problems early.

Singapore’s OCHA illustrates how this can work in practice. Authorities have issued binding directions to major platforms, including Meta, based on reasonable suspicion, before harmful content fully spreads<sup>35</sup>. This model directly addresses the speed problem by enabling intervention earlier than criminal prosecution would otherwise allow.

Any Cambodian framework would also need to distinguish between platform types and sizes, since smaller local platforms lack the capacity of large multinationals. A tiered approach, similar to the DSA’s distinction between very large platforms and smaller intermediaries, would impose proportionate obligations.

Several challenges remain. Enforcement capacity is the most significant: risk-assessment obligations are only meaningful if a regulator can evaluate compliance and impose consequences, and Cambodia does not yet have such a body. There is also a risk that large multinational platforms could disproportionately shape compliance frameworks to their advantage, burdening smaller Cambodian platforms with requirements designed around bigger players. Finally, Article 41 of the Constitution protects freedom of expression, meaning content-screening obligations must be carefully designed to avoid functioning as prior restraint<sup>36</sup>, and Cambodia’s regional obligations under the ASEAN Agreement on E-Commerce mean reforms diverging too far from regional norms could complicate cross-border digital trade<sup>37</sup>.

32 Delaney Hall, “*The ELIZA Effect*,” 99% Invisible, episode 382, 10 December 2019, <https://99percentinvisible.org/episode/the-eliza-effect/>.

33 Ministry of Post and Telecommunications (Cambodia), National Policy on Telecommunications 2020-2035 (Phnom Penh, 2020).

34 Regulation (EU) 2022/2065 (Digital Services Act), Arts. 16, 26, 30; Online Criminal Harms Act 2023 (Singapore), s. 7.

35 Meta Faces Review Under New Ocha Law After Spike in Government Impersonation Scams in Singapore, Malay Mail, 2 November 2025, <https://www.malaymail.com/amp/news/singapore/2025/11/02/meta-faces-review-under-new-ocha-law-after-spike-in-government-impersonation-scams-in-singapore/196898>.

36 Constitution of the Kingdom of Cambodia (1993, as amended), Art. 41.

37 ASEAN Framework Agreement on E-Commerce (Singapore, 22 January 2019), entered into force 2021.

## V. Conclusion

Cambodia's legal framework for digital platforms contains three structural gaps, (i) the absence of merchant verification obligations; (ii) the absence of a liability framework for AI-mediated psychological harm, particularly in the unregulated mental health service sector; and (iii) a predominantly reactive enforcement model. These gaps reflect a legal architecture that continues to treat platforms as passive intermediaries rather than active participants in the digital economy.

The EU's KYBC obligations, the UK's duty of care model, the EU AI Act's transparency requirements, Singapore's OCHA, and Vietnam's joint liability reforms differ in structure but converge on one principle, that platforms facilitate large-scale digital activity should bear proportionate obligations to prevent foreseeable harm. This gatekeeper logic is not radical; it mirrors obligations already imposed in banking, telecommunications, and pharmaceuticals.

Implementation in Cambodia does face real constraints. The system itself has underdeveloped verification infrastructure, no specialised digital regulator, unresolved causation doctrine for AI-mediated harm even in developed jurisdictions, and the risk that broad compliance obligations burden smaller platforms or expand state control over lawful speech. These limitations counsel a sequenced approach rather than no reform at all. KYBC obligations for high-volume platforms as a first step, paired with infrastructure investment, followed by the development of specialised regulatory capacity as AI-powered services expand further into Cambodia's economy.

A framework built for an era when platforms were passive conduits is no longer adequate to a digital economy in which platforms now mediate commerce, communication, and increasingly, emotional life. Cambodia's legal architecture must evolve accordingly.

## Bibliography

### International Legislation and Treaties

1. ASEAN Framework Agreement on E-Commerce. Singapore, 22 January 2019. Entered into force 2021.
2. Budapest Convention on Cybercrime, ETS No. 185. Council of Europe, 2001.
3. European Union. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive). OJ L178/1.
4. European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). OJ L277/1.
5. 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 (Artificial Intelligence Act). OJ L2024/1689.
6. Singapore. Online Criminal Harms Act 2023 (No. 24 of 2023). Commenced in part 1 February 2024.
7. United Kingdom. Online Safety Act 2023, c. 50.
8. United States. Communications Decency Act 1996, 47 U.S.C. Section 230.
9. Vietnam. Law on E-Commerce (amended), No. 20/2025/QH15. Promulgated 18 June 2025, effective 1 July 2026.

### National Legislation

1. Cambodia. Constitution of the Kingdom of Cambodia. 1993, as amended.
2. Cambodia. Cambodia Criminal Code. Promulgated 30 November 2009.
3. Cambodia. Law on Electronic Commerce,. Promulgated 16 November 2019.
4. Cambodia. Sub-Decree on E-Commerce Business Registration No. 65. 2021.
5. National Bank of Cambodia. Prakas on Know Your Customer (KYC) for Financial Institutions, B7-018-3 70. 2018.

### Case Law

1. Garcia v. Character Technologies, Inc. et al., No. 6:24-cv-01903-ACC-DCI (M.D. Fla., filed 22 October 2024), settled January 2026.

### Journal Articles

1. Buiten, Miriam, Alexandre De Streel, and Martin Peitz. 'The Economics of Platform Liability.' European Journal of Law and Economics 53 (2022): 1-31. <https://doi.org/10.1007/s10657-021-09718-x>.
2. Global Initiative Against Transnational Organized Crime. 'Cambodia's Role in Southeast Asia's Online Scam Epidemic.' Global Crime Perspective 3, no. 1 (2024). <https://doi.org/10.69131/GCP.03.01.2024.02>.

### Official Reports

1. Amnesty International. Cambodia: Authorities Failing to Act on Scam Compounds Despite Credible Evidence. 2023. <https://www.amnesty.org/en/latest/news/2023/09/cambodia-scam-compounds/>
2. General Department of Taxation (Cambodia). Revenue Report: E-Commerce Transactions January-July 2024. Phnom Penh: GDT, 2024.
3. Ministry of Home Affairs (Singapore). Provisions in the Online Criminal Harms Act on Codes of Practice and Implementation Directives to Come Into Force on 24 June 2024. Press Release, 21 June 2024.
4. Ministry of Post and Telecommunications (Cambodia). National Policy on Telecommunications 20-20-2035. Phnom Penh, 2020.
5. OECD AI Incident Monitor. Incident Report: Belgian Man Dies by Suicide Following AI Chatbot Conversations, Incident No. 2023-03-30-ab6d. 2023. <https://oecd.ai/en/incidents/incident-2023-03-30-ab6d>.
6. UNODC. Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Bangkok: UNODC ROSEAP, October 2024.





## **Legal Liability for Digital Service Providers in the Transportation Industry**

*LA Sophavann*

## Abstract

Digital service providers like Grab and TADA have reshaped Cambodia's transport sector and raised unresolved issues of tort liability. Although these platforms often claim intermediary protection under the Law on Electronic Commerce, their active involvement in pricing, driver management, payment processing, and service coordination suggests a level of operational control that may attract liability under Article 752 of the Civil Code.

Using doctrinal and comparative legal analysis, this study examines the overlap between the Civil Code's transportation liability rules and the electronic commerce intermediary regime, alongside applicable standards of care such as prudent management and digital due diligence. It also draws on the EU Digital Services Act to assess platform responsibility based on control and consumer perception. The study finds that Digital service provider are not purely passive intermediaries but functionally active service organizers. It argues that intermediary immunity should not apply where platforms exercise substantial control or where consumers reasonably perceive them as service providers. It proposes a Consumer Misconception Test and an authority-and-control framework to clarify Digital service provider liability in Cambodia's digital transport sector.

## I. Introduction

The rapid digital transformation of the Cambodian economy, marked by a surge to 19.7 million e-wallet accounts and a significant contribution to GDP by the E-Commerce sector<sup>1</sup>, has transformed how urban travel is organized and managed. In the transportation sector, traditional human dispatchers have been replaced by automated algorithms managed by Digital Service Providers ("DSP"), such as ride-hailing platforms like Grab and TADA. This shift has created a major gap in responsibility. While these platforms exert near-total control over the manner, means, and costs of a journey, they frequently frame themselves as mere technological intermediaries or software hosts to claim immunity from the liabilities traditionally imposed on transportation providers and employers. In Cambodia, where the regulatory framework for the digital economy is still developing through the Law on E-Commerce and the Law on Consumer Protection, this lack of clarity creates significant risks for passenger safety and consumer rights.

The main legal issue is whether a DSP operating a ride-hailing platform should be regarded merely as a protected intermediary under the Law on Electronic Commerce or as a primary transportation service provider under the Civil Code. This problem is subdivided into four sub-problems: (I) whether a DSP exercising substantial operational control may be considered a transportation manager under Article 752 of the Civil Code rather than a protected intermediary under the Law on Electronic Commerce; (II) whether DSPs owe a professional duty of care in driver vetting and safety supervision; (III) whether the notice-and-action obligations under the Law on Electronic Commerce require active intervention to prevent harm; and (IV) whether platform branding and consumer perception create independent grounds for liability under consumer protection law. By analyzing these issues through the lens of Cambodian statutes and international benchmarks like the EU Digital Services Act ("DSA"), this study will propose a superior solution adapted to Cambodia's technological context.

## II. Legal Classification of Digital Service Providers between Transportation Management and Intermediary Status

The threshold legal issue in the Cambodian transportation sector is the classification of the DSP's role. Traditionally, Cambodian law distinguishes between a private individual and a Professional Carrier, with the latter held to the standard of a Prudent Manager under Article 640 of the Civil Code.

In Cambodia, Article 752 of the Civil Code imposes liability on any person who owns or manages a transportation apparatus for harm caused to another<sup>2</sup>. While DSP does not physically own the vehicles in its network, it functionally satisfies the criteria of a manager through pervasive algorithmic control<sup>3</sup>. By setting non-negotiable fares, tracking mandatory GPS routes in real-time, and withholding passenger data from drivers, the DSP manages the entire service cycle rather than acting as a neutral host. This functional reality transforms the DSP into the manager, in fact, triggering a standard of presumed fault liability. Under this standard, the

1 National Bank of Cambodia, Annual Supervision Report 2023 (Phnom Penh: NBC,) p43, [https://www.nbc.gov.kh/download\\_files/publication/annual\\_rep\\_eng/NBC%20Annual%20Report%202023%20Eng.pdf](https://www.nbc.gov.kh/download_files/publication/annual_rep_eng/NBC%20Annual%20Report%202023%20Eng.pdf)

2 Civil Code of the Kingdom of Cambodia, Art. 752.

3 Jeremias Adams-Prassl, *Humans as a Service: The Promise and Perils of Work in the Gig Economy* (Oxford: Oxford University Press, 2018), pp.75-80. <https://global.oup.com/academic/product/humans-as-a-service-9780198797012>

law assumes the DSP is at fault for the accident, shifting the burden of proof to the platform; it can only rebut this presumption by proving it exercised the care of a Prudent Manager under Article 640 or that the harm resulted from unavoidable external circumstances<sup>4</sup>.

The central doctrinal issue is whether the concept of “management” under Article 752 should be confined to traditional physical control of a vehicle or interpreted more broadly to encompass digital forms of operational control. DSP may argue that it neither owns the vehicles nor physically operates them and therefore cannot be regarded as transportation managers within the meaning of Article 752<sup>5</sup>. Under this view, responsibility remains with the vehicle owner or driver who directly controls the transportation apparatus.

However, the operational structure of ride-hailing platforms suggests that DSP performs functions that extend beyond those of a passive intermediary. In practice, platforms determine fare structures, allocate passengers through proprietary algorithms, monitor journeys through GPS technology, establish service standards, process payments, manage customer complaints, and retain the authority to suspend or permanently deactivate drivers from the platform<sup>6</sup>. These functions enable DSPs to influence not only the commercial aspects of the service but also the manner in which transportation services are delivered to consumers<sup>7</sup>. Unlike a neutral technology provider that merely facilitates communication between independent parties, a DSP actively organizes and supervises the transportation network through digital means<sup>8</sup>.

For this reason, the question is not whether a DSP physically controls the vehicle, but whether its extensive economic and operational control over the transportation service constitutes a modern form of managerial authority. Although such control may not automatically render a DSP a transportation manager under Article 752, it provides a principled basis for arguing that the platform bears responsibilities comparable to those traditionally imposed on entities that organize and supervise transportation services.

This interpretation is supported by *Doe v. Uber Technologies, Inc.* (2016), where the court found that Uber exercised significant control over the transportation service through standardized fares, GPS monitoring, and driver deactivation powers. The court also emphasized passenger reliance on Uber’s representations regarding safety. Consequently, the platform’s role extended beyond that of a neutral intermediary and reflected a substantial degree of operational control over the service<sup>9</sup>.

DSP frequently attempts to bypass this management liability by invoking the “safe harbor provisions” of Article 24 of the Law on E-Commerce, which grants immunity to intermediaries providing services for storing or sending electronic records<sup>10</sup>. To resolve the conflict between the Civil Code’s mandate for responsibility and the E-Commerce Law’s grant of immunity, Cambodia should adopt the Consumer Misconception Test derived from Article 6(3) of the EU’s Digital Services Act. This standard specifies that intermediary immunity is nullified if a platform’s unified branding leads an average consumer to believe the service is being provided by the platform itself<sup>11</sup>. Therefore, the operational ride-hailing platforms like Grab and TADA suggest that they function beyond the role of passive intermediaries. Drawing on the analytical framework provided by the EU Digital Services Act, DSPs that exercise substantial control over the underlying transportation service may be subject to liability under Cambodian law rather than benefiting from intermediary immunity.

### III. Professional Standard of Care and Digital Due Diligence in Driver Vetting

Beyond being responsible for a driver’s physical actions, DSP in Cambodia faces direct tort liability for its own operational failures in network administration, driver onboarding, and ongoing supervision<sup>12</sup>. Safety policies and internal mitigation measures, including emergency hotlines, in-app safety buttons, and driver vetting protocols, are not merely optional commercial features; they constitute the evidentiary baseline for the Prudent Manager principle under Article 640 of the Civil Code<sup>13</sup>. Under Article 742(b), negligence is assessed by comparing an actor’s behavior to what a person with the “same profession or experience” could have foreseen and prevented. This establishes a heightened professional standard: as sophisticated technology firms, DSPs are legally expected to utilize their advanced data tools and superior technical knowledge to ensure that their safety policies are substantively effective rather than merely performative<sup>14</sup>.

4 Civil Code of the Kingdom of Cambodia, Art. 640.

5 Civil Code of the Kingdom of Cambodia, Art. 752.

6 Civil Code of the Kingdom of Cambodia, Art. 752.

7 Jeremias Adams-Prassl, *Humans as a Service: The Promise and Perils of Work in the Gig Economy* op. cit., pp.75–90.

8 Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford: Oxford University Press, 2016), pp.312-320; Martin Husovec, *Principles of Internet Intermediary Liability* (Oxford: Oxford University Press, 2023), pp.198-205. <https://global.oup.com/academic/product/the-liability-of-internet-intermediaries-9780198743941>

9 *Doe v. Uber Technologies, Inc.*, 184 F. Supp. 3d 774, 783-89 (N.D. Cal. 2016).

10 Law on Electronic Commerce of Cambodia, 2019, Art. 24.

11 Regulation (EU) 2022/2065 (Digital Services Act), Art. 6(3).

12 Civil Code of the Kingdom of Cambodia, Art. 747(2).

13 Civil Code of the Kingdom of Cambodia, Art. 640.

14 Civil Code of the Kingdom of Cambodia, Art. 747(2).

A primary operational failure involves the adequacy of background checks, necessitating the execution of proactive digital due diligence. While DSP may point to its onboarding policies as evidence of due care, the professional standard requires that these processes be rigorous enough to identify foreseeable risks. As demonstrated in *Doe v. Uber Technologies, Inc.* (2016), a professional entity is directly liable for negligent hiring if it “knew or should have known” of a driver’s unfitness. In that case, the court found that a background check failing to detect prior relevant convictions for assault constituted a breach of duty<sup>15</sup>. Similarly, if a Cambodian DSP implements a vetting mechanism but relies on an inadequate database that fails to detect a driver’s history of violence or dangerous driving, the platform remains directly liable; its specialized knowledge means it “should have known” the policy was insufficient to protect the public.

Furthermore, the duty of care extends to the active monitoring of safety devices and real-time supervision under Article 747(2) of the Civil Code. For a ride-hailing platform, the deployment of GPS tracking and emergency hotlines creates a continuous supervisory link between the platform and the driver<sup>16</sup>. If a DSP’s system identifies a safety flag, such as a driver repeatedly deviating from a prescribed GPS route or a passenger reporting a threat via an in-app SOS button, then the platform’s core legal obligation is to act as a proactive regulator. Under Article 25 of the Law on Electronic Commerce, once a platform has actual knowledge of a danger, it must act “immediately”<sup>17</sup>. Failure to expeditiously suspend a driver’s access once a risk becomes apparent through these internal safety tools directly violates the standard of a “Prudent Manager.” Consequently, safety policies do not serve as a shield against liability unless they are accompanied by diligent real-time enforcement, ensuring that fundamental rights to safety and human dignity are protected within the digital marketplace.

#### **IV. The Notice and Action Mandate: Statutory Obligations for Harm Mitigation**

The statutory boundaries of intermediary protection in Cambodia are further defined by the notice and action mandate established under the Law on Electronic Commerce. While Article 24 provides a general safe harbor for intermediaries, exempting them from liability for electronic records they did not originate, this immunity is conditional upon a lack of actual knowledge regarding illegal activity<sup>18</sup>. In the ride-hailing sector, DSPs frequently attempt to stretch this shield to cover physical harms; however, Article 25 imposes an active, non-delegable duty to act immediately upon becoming aware of information or events giving rise to civil or criminal liability<sup>19</sup>. In the transportation industry, this establishes a mandatory duty to deactivate. If a platform is notified of a dangerous incident, such as a driver threatening a passenger and fails to expeditiously disable the driver’s system access, it forfeits its statutory safe harbor protections and becomes directly liable for any resulting harm under both e-commerce and tort law.

This transition from a neutral host to a responsible provider is further informed by the authority and control exception derived from Article 6(2) of the EU’s Digital Services Act. Under this principle, liability exemptions shall not apply where the recipient of the service is acting under the authority or the control of the provider<sup>20</sup>. When a Cambodian DSP sets non-negotiable prices, prohibits drivers from collecting passenger contact details, and dictates the specific manner of service delivery via algorithms, it exerts a level of control that transforms it into a primary service provider rather than a passive broker<sup>21</sup>.

Holding DSP accountable for the physical execution of matched services is justified by the allocation of risk theory. This legal doctrine dictates that the entity which intentionally creates a zone of danger by matching strangers for profit, and which possesses the deep pockets necessary to provide redress, should bear the cost of harm<sup>22</sup>. Leaving victims to pursue individual drivers, who are frequently judgment-proof due to a lack of financial resources, would fail the fundamental purpose of tort law: to make the injured party whole again. Therefore, failure to fulfil the statutory mandate of Article 25 ensures that the DSP remains legally tied to the risks generated by its digital marketplace.

#### **V. The Branding Responsibility: Liability Arising from Consumer Misconception**

The last sub-issue of core DSP responsibility involves the legal consequences of unified branding and market presentation under the Law on Consumer Protection and the Civil Code. While DSP often claims status as mere software hosts to evade responsibility, it frequently mandates that drivers wear company uniforms, display platform stickers on their vehicles, and

15 *Doe v. Uber Technologies, Inc.*, 184 F. Supp. 3d 774, 783-89 (N.D. Cal. 2016).

16 Civil Code of the Kingdom of Cambodia, Art. 747(2).

17 Law on Electronic Commerce of Cambodia, 2019, Art. 25.

18 Law on Electronic Commerce of Cambodia, 2019, Art. 24.

19 Law on Electronic Commerce of Cambodia, 2019, Art. 25.

20 Regulation (EU) 2022/2065 (Digital Services Act), Art. 6(2)

21 *Doe v. Uber Technologies, Inc.*, 184 F. Supp. 3d 774 (N.D. Cal. 2016).

22 Steve Hedley and Nicola Padfield, *Tort*, 7th ed. (Oxford: Oxford University Press, 2011), p. 70.



adhere to a digital interface that exclusively features the platform's brand. Under Articles 10, 11, and 12 of the Law on Consumer Protection, business operators are strictly prohibited from engaging in misleading representations regarding the nature, characteristics, or quality of a service<sup>23</sup>. By marketing a unified "Grab" or "TADA" experience, the platform creates a commercial expectation of safety and reliability that leads passengers to believe they are entering a vetted corporate vehicle rather than a private car driven by an unmanaged individual. This brand-induced trust creates a legal obligation under Article 13 of the Civil Code, which grants victims the right to seek damages when such personal safety and dignity expectations are breached<sup>24</sup>.

To resolve the conflict between technological safe harbors and physical harm, Cambodia should adopt the Consumer Misconception Test derived from Article 6(3) of the EU's Digital Services Act<sup>25</sup>. This principle establishes that liability exemptions shall not apply if a platform presents information or enables a transaction in a way that would lead a reasonably well-informed and reasonably observant internet user to believe the service is provided by the platform itself. This standard ensures that if a platform's branding and integrated services such as managing the entire payment cycle and GPS tracking make it indistinguishable from a primary provider, it must remain liable for service failures<sup>26</sup>. In the Cambodian context, where digital literacy is still developing, estimated at only 5% at an intermediate level, consumers rely even more heavily on these high-visibility brands as a guarantee of integrity<sup>27</sup>. Consequently, any physical harm occurring during execution becomes the liability of the DSP as the perceived provider, ensuring that the entity which profits from the trust generated by its brand also bears the allocation of risk for that service's failure.

A primary example of this principle within the transportation industry is the landmark case of *Doe v. Uber Technologies, Inc.* (2016). In this case, the court examined whether a platform's branding and public messaging regarding safety created a specific duty of care toward its passengers. The court noted that because Uber's services are available to the general public and the platform charges standardized, non-negotiable fees, it functions as a common carrier rather than a passive technological broker. Crucially, the court found it reasonable to infer that passengers accept rides from drivers in direct reliance on the platform's stamp of approval and its representations of safety<sup>28</sup>. Similarly, in *Rogers v. Night Riders*, it was established that a minicab service could not plead that its drivers were independent contractors once it had deliberately fostered a commercial impression that it was responsible for the passengers' safety<sup>29</sup>. These transportation-specific precedents demonstrate that branding is not merely a marketing tool but a source of legal responsibility that ties the platform to the physical safety of its users under both consumer protection and tortious principles.

## VI. Conclusion

The legal landscape for transportation in Cambodia is currently caught in a tension between the traditional definitions of transportation managers and the modern status of DSP as intermediaries. While ride-hailing platforms like Grab and TADA often invoke safe harbor protections under Article 24 of the Law on Electronic Commerce to claim immunity, their functional reality involves total algorithmic control over the service cycle, including pricing, real-time GPS tracking, and driver deactivation. This control aligns their activities with the definition of a manager under Article 752 of the Civil Code, which imposes presumed fault liability for harms caused during the operation of a transportation apparatus.

The main solution to bridge this responsibility gap is for Cambodian lawmakers and courts to adopt the Consumer Misconception Test derived from Article 6(3) of the EU's Digital Services Act. This standard stipulates that a platform's immunity is nullified if its unified branding, such as uniforms, stickers, or centralized payments, leads a reasonable consumer to believe the service is being provided by the platform itself. Additionally, an authority and control exception should be codified to ensure that platforms managing the physical service cycle are held to a professional standard of care under Article 742 of the Civil Code. This requires platforms to perform rigorous digital due diligence in driver vetting and real-time safety monitoring to protect the fundamental rights to safety and human dignity.

23 Law on Consumer Protection of Cambodia, Art. 10-12.

24 Civil Code of the Kingdom of Cambodia, Art. 13.

25 Regulation (EU) 2022/2065 (Digital Services Act), Art. 6(3).

26 *Christian Louboutin SAS v. Amazon Europe Core Sàrl*, Joined Cases C-148/21 and C-184/21, Court of Justice of the European Union, 22 December 2022.

27 UNESCO, "Cambodia Launches Its First Competency Framework on Digital, Media and Information Literacy," July 4, 2024.

28 *Doe v. Uber Technologies, Inc.*, 184 F. Supp. 3d 774 (N.D. Cal. 2016).

29 *Rogers v. Night Riders*, [1983] RTR 324 (QBD), [https://www.uni-goettingen.de/de/document/download/40331bd-35f7aee1be4eec6bc25471f89.pdf/14.%20%20Strict%20Liability%20\(Session%206\).pdf](https://www.uni-goettingen.de/de/document/download/40331bd-35f7aee1be4eec6bc25471f89.pdf/14.%20%20Strict%20Liability%20(Session%206).pdf)



## Bibliography

### Laws and Regulations

1. Civil Code of Cambodia, NS/RKM/1207/031, 5 October 2007.
2. Law on Consumer Protection of Cambodia, NS/RKM/1119/016, 2 November 2019.
3. Law on Electronic Commerce of Cambodia, NS/RKM/1119/017, 2 November 2019.
4. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).

### Case Laws

1. *Christian Louboutin SAS v. Amazon Europe Core Sàrl*, Joined Cases C-148/21 and C-184/21, Court of Justice of the European Union, 22 December 2022.
2. *Doe v. Uber Technologies, Inc.*, 184 F. Supp. 3d 774 (N.D. Cal. 2016).
3. *Rogers v. Night Riders*, [1983] RTR 324 (QBD).

### Books and Journal Articles

1. Adams-Prassl, Jeremias. *Humans as a Service: The Promise and Perils of Work in the Gig Economy*. Oxford: Oxford University Press, 2018.
2. Hedley, Steve, and Nicola Padfield. *Tort*. 7th ed. Oxford: Oxford University Press, 2011.
3. Husovec, Martin. *Principles of Internet Intermediary Liability*. Oxford: Oxford University Press, 2023.
4. Riordan, Jaani. *The Liability of Internet Intermediaries*. Oxford: Oxford University Press, 2016.
5. Busch, Christoph. "Self-Regulation and Regulatory Intermediation in the Platform Economy." *European Business Organization Law Review* 20, no. 1, 2019: pp.93-126.
6. Frosio, Giancarlo. "Reforming Intermediary Liability in the Platform Economy." *Oxford Journal of Legal Studies* 37, no. 3, 2017: pp.1-29.
7. Lobel, Orly. "The Law of the Platform." *Minnesota Law Review* 101, no. 1, 2016: pp.87-166.
8. Ranchordás, Sofia. "Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy." *Minnesota Journal of Law, Science & Technology* 16, no. 1, 2015: pp.413-475.
9. Van Cleynenbreugel, Pieter. "Platform Liability and the Digital Services Act." *Common Market Law Review* 59, no. 6, 2022: pp.1635-1668.

### Reports

1. National Bank of Cambodia. "Annual Supervision Report 2023". Phnom Penh: National Bank of Cambodia, 2024.
2. UNESCO. "Cambodia Launches Its First Competency Framework on Digital, Media and Information Literacy." 4 July 2024.

### Websites

1. Grab Cambodia. "Transport, Delivery and Logistics Terms & Policies." Accessed 20 June 2026. <https://www.grab.com/kh/en/terms-policies/transport-delivery-logistics/>.

## News Articles

1. 'Google and Character.AI Agree to Settle Lawsuit Linked to Teen Suicide.' JURIST, 8 January 2026. <https://www.jurist.org/news/2026/01/google-and-character-ai-agree-to-settle-lawsuit-linked-to-teen-suicide/>.
2. International Consortium of Investigative Journalists. 'Cambodian Payment Processor Freezes Customer Funds Before Regulators Shut It Down.' 9 December 2025. <https://www.icij.org/investigations/coin-laundry/cambodian-payment-processor-freezes-customer-funds-before-regulators-shut-it-down/>.
3. 'Meta Faces Review Under New Ocha Law After Spike in Government Impersonation Scams in Singapore.' Malay Mail, 2 November 2025. <https://www.malaymail.com/amp/news/singapore/2025/11/02/meta-faces-review-under-new-ocha-law-after-spike-in-government-impersonation-scams-in-singapore/196898>.
4. Nelson, Danny, and Camomile Shumba. 'Sanctioned Cambodian Lender Huione, Linked to Illicit Crypto, Faces Bank Run.' CoinDesk, 2 December 2025. <https://www.coindesk.com/policy/2025/12/02/sanctioned-cambodian-bank-huione-halts-business-after-mass-run-on-accounts-report>.
5. US Department of the Treasury, Financial Crimes Enforcement Network. Imposition of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern. 90 Fed. Reg. 18942, 5 May 2025. <https://www.federalregister.gov/documents/2025/05/05/2025-07837/>.
6. Coeckelbergh, Mark. 'Chatbots Can Kill.' Medium, 29 March 2023. <https://coeckelbergh.medium.com/chatbots-can-kill-d82fde5cf6ca>.
7. Delaney Hall, "The ELIZA Effect," 99% Invisible, episode 382, 10 December 2019, <https://99percentinvisible.org/episode/the-eliza-effect/>.



## **The Legal Implications of Deferred Equity: Reforming Cambodia's Legal Framework for Startup Equity Compensation**

*SE Chhunlim*

## Abstract

Cambodia's ambition to develop a digitally driven economy has placed startup growth in an important position of its national policy agenda. However, its legislative system governing labor remuneration, taxation, and corporate structure were enacted without any contemplation of equity-based compensation. This paper argues that three deficiencies exist under Cambodian law that render Employee Share Option Plan (“ESOP”), which are the primary equity compensation mechanism relied upon by startups, legally untenable. The Labor Law's broad wage definition, the Fringe Benefit Tax (“FBT”) regime under Prakas No. 575 on Tax on Salary (“Prakas No. 575”), and the thirty-shareholder ceiling under the Law on Commercial Enterprise (“LCE”) collectively highlight that the current legal system in Cambodia has failed to recognize equity-based compensation as a distinct legal instrument, leaving startups without a clear legal foundation to sustain their equity compensation arrangements. Drawing on comparative models from France and Singapore, this paper proposes four legal reforms to close this gap.

## I. Introduction

Cambodia is currently undergoing a transition toward a more innovative and digitally driven economic model and as such the growth of startups is considered a key governmental priority<sup>1</sup>. Contrary to standard businesses, startup capital is raised through the issuance of company shares; where employees are often compensated through equity-based incentive rather than immediate cash remuneration<sup>2</sup>. The standard compensation arrangement for startups is an ESOP, in which the employee accepts below-market cash wages in exchange for vesting rights over company shares<sup>3</sup>. In other words, employees, in addition to their cash wages, could be compensated through receiving company shares outright or being granted stock options, which gives them the right to buy company shares at a fixed price after a certain period of time. This structure is designed to function as an employee retention mechanism that is vital to startups<sup>4</sup>.

However, this startup equity-based compensation plan collides with the following areas of law being the Labor Law of Cambodia (“**Labor Law**”<sup>5</sup>), which governs employee remuneration and employment benefits; Prakas No. 575 on Tax on Salary, which concerns how equity based compensation are to be taxed<sup>6</sup>; and the LCE<sup>7</sup>, which governs corporate capital structure; revealing a structural incompatibility between the country's existing regulations and the operational realities of startup enterprises<sup>8</sup>.

This paper explores the challenges arising from the inability of Cambodia's existing legal framework to accommodate the startup equity, scoping down into three interlocking sub-problems by exploring (II) the conflict between overtime pay and the deferred equity compensation structures that startups use to attract and maintain talent; (III) The FBT Liquidity Trap: Employer Burden Under Prakas No. 575; and the (IV) thirty shareholders limit affecting the startup structure.

## II. The Conflict Between Overtime Pay and the Deferred Equity Compensation Structures That Startups Use to Attract and Maintain Talent

The core issue under the Labor Law is that wages are defined as “remuneration for the employment or service set by agreement between the parties” and includes “the values of benefits in kind<sup>9</sup>”. Following this standard, ESOPs would fall under the category of being part of an employee's wage<sup>10</sup>. With overtime pay

1 Supreme National Economic Council, Cambodia Digital Economy and Society Policy Framework 2021–2035, pp. 2–3 (2021).

2 Andrea L. Eisfeldt, Antonio Falato, and Mindy Z. Xiaolan, “*Human Capitalists*,” NBER Working Paper No. 28815 (National Bureau of Economic Research, May 2021, revised April 2022), pp. 1–2.

3 National Center for Employee Ownership (“NCEO”), “*What Is Employee Ownership?*”, NCEO, available at: <https://www.nceo.org/what-is-employee-ownership/esop-employee-stock-ownership-plan>

4 OECD, The Taxation of Employee Stock Options, OECD Tax Policy Studies, No. 11 (Paris: OECD Publishing, 2005), 11, <https://doi.org/10.1787/9789264012493-en>.

5 Labor Law, Royal Kram No. CS/RKM/0397/01, March 13, 1997, as amended 2007, 2018, and 2021

6 Prakas No. 575 MEF.P.GDT on Tax on Salary, issued by the Ministry of Economy and Finance (MEF), dated September 19, 2024.

7 Law on Commercial Enterprise, Royal Kram No. NS/RKM/0505/009, dated May 19, 2005, as amended by Royal Kram NS/RKM/0122/002, dated January 29, 2022

8 Supreme National Economic Council, Cambodia Digital Economy and Society Policy Framework 2021–2035, pp. 22–23.

9 Art. 102 of Labor Law.

10 Seng Chanvireak, “*Cambodia Employee Stock Options: A Strategic Guide*,” Lawyering As Code, October 5, 2025. [https://lawyeringascode.com/posts/12\\_cambodia\\_employee\\_stock\\_options\\_overview/](https://lawyeringascode.com/posts/12_cambodia_employee_stock_options_overview/).



having to be calculated for employee wages, employers would then be legally required to calculate their overtime rates (which ranges from 150% to 200% of their normal wage) based on the Labor Law<sup>11</sup>. As a result, the mandatory conversion of overtime remuneration into equity could force employers to issue shares that exceed their authorized capitalization. Although a reasonable counterargument is that overtime equity payments could be settled in cash equivalent to the share value per contractual agreement. Nonetheless, this is unfeasible for startups as the companies are relying on below-market cash wages because they are cash-constrained, and converting equity to shares defeats the purpose of deferring equity compensation in the first place. These issues are precisely why practitioners have argued that ESOPs should be categorized as a category separate from wages<sup>12</sup>.

Here, France serves as a strong comparative model because the Cambodian legal system is largely based on the French civil law tradition making integration feasible without facing major legal hurdles<sup>13</sup>. In fact, France had faced the same legal problem as to whether ESOPs would be considered as an employee's wage, in the case of *Google France v. [G]* (Cass. soc.), the Supreme Court of France held that neither free shares nor stock options count toward that base<sup>14</sup>. This holding is reinforced by the fact that ESOPs fall into the category of free shares *Attributions Gratuites d'Actions* ("AGA") under the Commercial Code, rather than the French Labor Code<sup>15</sup>. The AGA framework establishes a regulated structure, capping employee free share grants at 15% of share capital generally, rising to 20% for qualifying small and medium enterprises, and as high as 30% to 40% where the grant extends broadly across the workforce<sup>16</sup>. This imposed limitation on employee shares helps protect investors and shareholders from excessive capital dilution while also promoting employee equity. Generally, as the stock option pool for startup employees ranges around 10% to 15%<sup>17</sup>, this regulation does not impose a heavy restriction for startup enterprises. Additionally, because AGA's vesting and structural requirements are rooted in corporate law rather than employment law, the instrument is isolated from being categorized as wages, which in turn ensures that French companies are not forced to treat equity compensation as part of the wage base used to calculate overtime.

By adopting a similar regulatory regime in Cambodia, whereby employee shares do not constitute as a "wage" under the Labor Law which could be done by amending Article 103 of the Labor Law to add equity-based compensation into an already existing exception clause of instruments that do not fall into the definition of wages, and with considerations of imposing a legal cap on the employee share option pool, this framework ensures the functionality of startup enterprises by allowing them to use ESOPs as intended, rather than as a liability.

### III. The FBT Liquidity Trap: Employer Burden Under Prakas No. 575

Generally, ESOPs follow four key stages: the date of the grant, the vesting period, the date of exercise, and the sale of the shares acquired<sup>18</sup>. The date of the grant refers to the day a company formally offers an employee the right to purchase a specific number of company shares at a predetermined price<sup>19</sup>. The vesting period is the minimum holding period between the grant date and the point at which the employee earns the right to exercise their share options<sup>20</sup>; the date of exercise, which is when employees choose to buy the shares at the locked-in exercise price set at grant; and the sale of the shares is when the employee sells those shares on the open market<sup>21</sup>.

The 20% FBT presents one of the most significant regulatory obstacles to the implementation of ESOPs in Cambodia. According to Prakas No. 575, issued by the Ministry of Economics and Finance (MEF), the company shares or stock options granted to an employee would fall under a "taxable fringe benefit<sup>22</sup>", which imposes a 20% FBT liability on the employer<sup>23</sup>. As equity compensation granted to employees would be treated as

11 Arts. 137-140 of Labor Law.

12 Seng Chanvireak, "Cambodia Employee Stock Options: A Strategic Guide," *Lawyering As Code*, October 5, 2025, [https://lawyeringascode.com/posts/12\\_cambodia\\_employee\\_stock\\_options\\_overview/](https://lawyeringascode.com/posts/12_cambodia_employee_stock_options_overview/).

13 Kong Phallack, "Overview of the Cambodian Legal and Judicial System," in *Introduction to Cambodian Law*, ed. Hor Peng, Kong Phallack, and Jörg Menzel, Konrad-Adenauer-Stiftung, 2012, p. 7.

14 France, Cour de cassation [Cass.] [Supreme Court] soc., November 15, 2023, No. 22-12.501, para. 12.

15 Arts. L. 225-197-1 to L. 225-197-6 of Commercial Code.

16 *Ibid.*

17 Yifat Aran, "Making Disclosure Work for Start-Up Employees," *Columbia Business Law Review* 2019, no. 3 (2019): pp. 95-96.

18 OECD, "The Taxation of Employee Stock Options", OECD Tax Policy Studies, No. 11, OECD Publishing, 2005, p. 10, available at: <https://doi.org/10.1787/9789264012493-en>.

19 *Ibid.*

20 *Ibid.*

21 *Ibid.*

22 Arts. 15(2)(n) of Prakas No. 575 on Tax on Salary.

23 Art. 17 of Prakas No. 575 on Tax on Salary.



a fringe benefit, set at a tax rate at 20% of its total value that is taxed monthly<sup>24</sup>, placing the taxable burden on the employer would be especially prejudicial to early-stage startups. For a startup using standard ESOPs, this would mean a recurring tax obligation, requiring startups to pay a 20% tax on the estimated value of the share of all active ESOPs. Since startups grant equity in place of cash salary because they lack the cash to begin with, the current FBT creates an ongoing compounding drain on liquidity precisely when the company is least equipped to absorb it, potentially harming the growth of startups.

Comparatively, Singapore's ESOP tax framework emphasizes that a clear valuation methodology can work effectively without complex legislation; and as a fellow ASEAN member state, Singapore's legislative model offers regional compatibility, giving Cambodia a pragmatic model that balances startup growth interests with current tax laws in a manner suited to Cambodia's current legal system. In Singapore, the Income Tax Act (ITA) places the tax burden on the employee and does not tax employee stock options when they're granted but rather when the options are exercised<sup>25</sup>. This eliminates the liquidity problem entirely. The employer has no FBT obligation at all, meaning a startup is not forced to pay cash tax on equity it has handed out while it is still trying to grow. Furthermore, by the time the employee exercises the options, they are choosing to do so because it makes financial sense, meaning the shares are worth more than the exercise price. At the point of exercise, a real and quantifiable gain exists, and the employee is therefore in a position to bear the corresponding tax liability. For startups, this is an arguably better alternative as it places the tax burden on the party that receives the benefit at the point of exercise rather than the startup which has to pay a substantial cash tax on a stock option when the employer has not received any actual cash from the equity.

Resolving this would require consideration for an amendment to be made on Prakas No. 575. Firstly, Prakas No. 575 should be amended to remove the monthly recurring FBT obligation on equity compensation entirely. Under the current structure, treating share grants as a monthly fringe benefit forces startups to continuously calculate and pay tax on unvested shares that have not yet produced any tangible benefit for either party. Instead, the taxable event should be deferred to the point of exercise, following Singapore's approach whereby tax is only triggered when the employee actually realises a gain from their options. Secondly, Prakas No. 575 should be amended to move the tax burden towards the employee rather than the employer as early stage startups may struggle to provide liquidated cash on an equity-based transaction, in which the employee receives the benefit, ensuring a sustainable regime for start-up enterprises.

#### IV. The Thirty-Shareholder Ceiling Conflicting with Startup ESOPs

Article 86 of the LCE caps a private limited company with thirty shareholders<sup>26</sup>. An enterprise that exceeds thirty holders falls outside the private limited company altogether. As such, employee ESOPs would fall under this category, and every employee shareholder would then need to be registered in the article of incorporation<sup>27</sup>. Within a few years, employees with ESOPs could take up the majority of the shareholder spots before investors are even counted<sup>28</sup>. The LCE offers no employee-share exemption, causing an issue for startups, limiting their ability to offer shares especially in a talent-scarce market.

Although the alternative would be to convert to a public limited company under Article 87 and 91<sup>29</sup>, public limited companies face bigger restrictions and legal hurdles such as: requiring three directors, an auditor it can no longer decline to appoint, the heightened financial-disclosure duties of Article 224 to 234 (including filing their accounts with the Director of Companies and opening their records to public inspection), and, on any public offer of securities, oversight by the Securities and Exchange Regulator of Cambodia (SERC) under the separate Securities Law<sup>30</sup>. Imposing that burden on an early-stage startup company merely to accommodate employee options is disproportionate, and it dismantles the flexible structure that makes private limited companies attractive for startups.

Singapore, the undisputed hub for Southeast Asian venture capital and the jurisdiction against which corporate frameworks are measured<sup>31</sup>, addresses the same problem expressly. As both Cambodia and Singapore

<sup>24</sup> *Ibid.*

<sup>25</sup> Section 10(6)(a) of the Income Tax Act Singapore.

<sup>26</sup> Art. 86 of Law on Commercial Enterprise,

<sup>27</sup> Art. 93(i) of Law on Commercial Enterprise,

<sup>28</sup> Henry Yin, Benjamin Yao, Bowen Yang, Shaun Tho, Michael Gerald, and Marina Casani. "Understanding Employee Stock Ownership Plans: Legal Considerations Across Key Asia Jurisdictions." Loeb & Loeb LLP, January 2024. available at: <https://www.loeb.com/en/insights/publications/2024/01/understanding-employee-stock-ownership-plans-legal-considerations-across-key-asia-jurisdictions>.

<sup>29</sup> Arts. 87 and 91 of Law on Commercial Enterprise,

<sup>30</sup> Arts. 118, 224-234 of LCE; Arts. 12, 16, Law on the Issuance and Trading of Non-Government Securities (2007).

<sup>31</sup> PitchBook and Pacific Basin Economic Council, 2024 Southeast Asia Private Capital Breakdown (May 2024), p. 5, available at: [https://www.pbec.org/wp-content/uploads/2024/05/2024\\_Southeast\\_Asia\\_Private\\_Capital\\_Breakdown-Pitchbook.pdf](https://www.pbec.org/wp-content/uploads/2024/05/2024_Southeast_Asia_Private_Capital_Breakdown-Pitchbook.pdf).

are economies that rely heavily on attracting foreign direct investment to grow, this makes Singapore's legal solutions directly relevant to Cambodia's ongoing challenges<sup>32</sup>. Under Singapore's Company Act, shares held by employees under an employee scheme from private-company members are exempt from counting towards the shareholder ceiling, so that employee ownership does not force conversion to public status<sup>33</sup>. This allows startups in Singapore to thrive by ensuring that ESOPs remain a viable mechanism for attracting talent, without worry of heavy administrative and financial burdens of an early public conversion. Singapore allows startups to scale their workforce and reward employees with equity freely, without that growth pushing them out of the private company structure they depend on to operate flexibly with minimal restrictions.

Here, a targeted amendment to Article 86 of the LCE should therefore be introduced to exclude shares issued under the official employee equity plan to not count towards the 30 shareholders limit. Such a change would resolve the incompatibility between the LCE and startup equity compensation by allowing startups to grant equity broadly across their workforce while preserving shareholder slots for investors, whose participation is equally essential to the startup's growth and survival. Without this exception, every employee shareholder replaces a potential investor, forcing startups to choose between retaining talent and raising capital. This amendment does not need a complete restructure of the LCE, Cambodia only needs to introduce a clearly defined exception that reflects the operational realities of startups to ensure that these enterprises are able to attract and retain talent while ensuring their survivability and capital.

## V. Conclusion

As this brief has shown, Cambodia's startup ecosystem is constrained by a legal system that was never designed with equity-based compensation in mind. Three points of friction highlight this incompatibility. First, under the Labor Law, the current definition of wages would include equity-based compensation programs, potentially including ESOPs in overtime pay, risking share dilution and turning equity-based compensation programs into liabilities for startups. Second, Prakas No. 575 provides that employers must pay out the benefits in cash even though the equity being granted generates no immediate cash income, creating more financial burden on the startup. Third, the LCE, the thirty shareholder limit counts employee shareholders alongside investors, potentially pushing a growing startup out of the private limited form if it wants to retain employees while having adequate investors for the enterprise.

To close this gap, Cambodia should pursue targeted reforms by amending the relevant provisions of the Labor Law to exclude ESOPs from the wage definition and consider amendments to cap the employee share option pool. Moreover, Prakas No. 575 should be considered to remove the monthly FBT obligation on employers in respect of equity-based compensation and instead deferring the taxable event to the point of exercise paid by the employee. Lastly, an exception to Article 86 of the LCE regarding the shareholder limit should be carved out to exclude employee shares issued under the official employee equity plan. None of these reforms requires an overhaul of Cambodia's broader legal system, only adjustments that bring the law in step with how startups operate. By adopting them, Cambodia can align its legal framework with the operational realities of equity-based compensation, positioning its startup ecosystem for sustained growth and stronger competitiveness within the region.

---

32 Del Rosario, Diana, Hoang Nam Nguyen, and Li Lian Ong. "The Reconfiguration of Foreign Direct Investment in ASEAN+3." AMRO Working Paper WP/24-13. Singapore: ASEAN+3 Macroeconomic Research Office, October 2024, p.16.

33 s. 18(1)(b). of Singapore Companies Act 1967 (Cap. 50),

## Bibliography

### Legislation and Regulations

1. Labor Law of Cambodia, Royal Kram No. CS/RKM/0397/01, dated March 13, 1997, as amended 2007, 2018, and 2021.
2. Law on Commercial Enterprises, Royal Kram No. NS/RKM/0505/009, dated May 19, 2005, as amended by Royal Kram NS/RKM/0122/002, dated January 29, 2022.
3. Prakas No. 575 MEF.P.GDT on Tax on Salary, issued by the Ministry of Economy and Finance (MEF), dated September 19, 2024.
4. France, Commercial Code.
5. Singapore Companies Act 1967.
6. Singapore Income Tax Act 1947.

### Cases

1. France, Cour de cassation [Cass.] [Supreme Court] soc., November 15, 2023, No. 22-12.501.

### Books, Reports, and Working Papers

1. Del Rosario, Diana, Hoang Nam Nguyen, and Li Lian Ong. "The Reconfiguration of Foreign Direct Investment in ASEAN+3." AMRO Working Paper WP/24-13. Singapore: ASEAN+3 Macroeconomic Research Office, October 2024.
2. Eisfeldt, Andrea L., Antonio Falato, and Mindy Z. Xiaolan. "Human Capitalists." NBER Working Paper No. 28815. National Bureau of Economic Research, May 2021, revised April 2022.
3. Hor Peng, Kong Phallack, and Jörg Menzel, eds. Introduction to Cambodian Law. Phnom Penh: Konrad-Adenauer-Stiftung, 2012.
4. OECD. The Taxation of Employee Stock Options. OECD Tax Policy Studies, No. 11. Paris: OECD Publishing, 2005. <https://doi.org/10.1787/9789264012493-en>.
5. PitchBook and Pacific Basin Economic Council. 2024 Southeast Asia Private Capital Breakdown. May 2024. [https://www.pbec.org/wp-content/uploads/2024/05/2024\\_Southeast\\_Asia\\_Private\\_Capital\\_Breakdown-Pitchbook.pdf](https://www.pbec.org/wp-content/uploads/2024/05/2024_Southeast_Asia_Private_Capital_Breakdown-Pitchbook.pdf).
6. Supreme National Economic Council. Cambodia Digital Economy and Society Policy Framework 2021–2035. Phnom Penh: Royal Government of Cambodia, 2021.

### Journal Articles

1. Aran, Yifat. "Making Disclosure Work for Start-Up Employees." Columbia Business Law Review 2019, no. 3 (2019): 95–96.

### Website

1. National Center for Employee Ownership. "What Is Employee Ownership?" NCEO. <https://www.nceo.org/what-is-employee-ownership/esop-employee-stock-ownership-plan>.
2. Seng, Chanvireak. "Cambodia Employee Stock Options: A Strategic Guide." Lawyering As Code, October 5, 2025. [https://lawyeringascode.com/posts/12\\_cambodia\\_employee\\_stock\\_options\\_overview/](https://lawyeringascode.com/posts/12_cambodia_employee_stock_options_overview/)
3. Yin, Henry, Benjamin Yao, Bowen Yang, Shaun Tho, Michael Gerald, and Marina Casani. "Understanding Employee Stock Ownership Plans: Legal Considerations Across Key Asia Jurisdictions." Loeb & Loeb LLP, January 2024. <https://www.loeb.com/en/insights/publications/2024/01/understanding-employee-stock-ownership-plans-legal-considerations-across-key-asia-jurisdictions>.



## When Digital Data Drives Market Power: Evaluating Cambodia's Compensation Framework for App-Based Mobility Services

NHETH Vichetneath

## Abstract

The rapid rise of app-based mobility services in Cambodia have not only reshaped its urban transport system but have also introduced new forms of digital market power. These powers – specifically the network effects, data control, and algorithmic pricing – aggravates unfair competition practices and raises concerns regarding the ability of existing legal frameworks to effectively respond. Cambodia's current competition framework – particularly the Law on Competition (2021) – is a non-digital specific competition law regime, which remains vague and largely relies on ex-post regulatory tools that limits its ability to address the abuse of dominance in digital markets. This brief argues for the issuance of digital-specific guidelines, the adoption of a multi-factor test for the assessment of digital dominance, the strengthening of ex-ante regulatory tools, and examines the applicability of the EU's Digital Markets Act for Cambodia, to balance digital innovation against fair competition practices in its digitally evolving mobility sector.

## I. Introduction

Unlike the Big Bad Wolf, big is not necessarily bad in competition law. It is a misconception that large firms are inherently problematic, as competition law does not condemn size, but rather, the misuse of market power. The challenge, however, lies in identifying such misuse when the governing competition law framework has yet to evolve to regulate it effectively.

In Southeast Asia's urban cities, informal transport services fill the accessibility gaps left by the underinvestment in public transportation systems and the lack of infrastructure<sup>1</sup>. Ride-hailing platforms have emerged as a popular part of this informal network, reshaping mobility options across the region.

At the same time, this region has experienced strong urban population growth, rising incomes, and dramatic improvement of digital connectivity in recent years, accelerating the demand for app-based mobility. Cambodia in particular, saw mobile cellular subscriptions rise to 116 out of every 100 individuals in 2024<sup>2</sup>, reflecting a widespread digital adoption. Although these statistics are relatively low compared to neighboring countries in Southeast Asia<sup>3</sup>, Cambodia has seen the rapid emergence and adoption of app-based mobility services. This growth has been driven by both technological readiness and dissatisfaction with existing public transportation systems. In Phnom Penh especially<sup>4</sup>, app-based mobility services have delivered significant efficiencies, cementing themselves as an integral part of the urban transport system.

Following this trajectory, the rise of dominant digital platforms in app-based mobility markets<sup>5</sup> raises questions about whether existing legal frameworks are capable of addressing and regulating new forms of market power – specifically, the network effects, data control, and algorithmic pricing that lock in users and drivers. These dynamics aggravate beyond traditional competition concerns (such as exclusionary conduct), and also create new challenges that are unique to the digital markets. In Cambodia, there are regulatory frameworks for app-based mobility services remain light-touch, focusing largely on business and vehicle registration and safety. There are also existing frameworks that regulate market competition. Yet, as of the time this brief is written, Cambodia does not have any legal instruments regulating competition at the intersection between the two.

This gap poses an inherent problem going forward, as generally, dominant digital platforms derive market power from their control over user data<sup>6</sup>, allowing for network effects and algorithmic pricing strategies to be deployed.

1 Saksith Chalermpong, Hironori Kato, Phathinan Thaitatkul, Apiwat Ratanawaraha, Alexis Fillone, Nguyen Hoang Tung, and Peraphan Jittrapirom, "Ride hailing applications in Southeast Asia: A literature review," International Journal of Sustainable Transportation, published online 2022, available at: <https://doi.org/10.1080/15568318.2022.2032885>.

2 World Bank, "Mobile cellular subscriptions (per 100 people)," World Development Indicators, n.d., available at: <https://data.worldbank.org/indicator/IT.CEL.SETS.P2>.

3 International Transport Forum (ITF), Regulating app based mobility: Case Studies from Bangkok, Manila, and Phnom Penh, International Transport Forum Policy Papers, No. 139 (Paris: OECD Publishing, 2024), pp. 7–13.

4 Pascal Medeville, "Revolution on the Road: The Rise of Ride Hailing Apps in Cambodia," Wonders of Cambodia, February 23, 2026, available at: <https://wondersofcambodia.com/revolution-on-the-road-the-rise-of-ride-hailing-apps-in-cambodia/>.

5 Ekalavya Hansaj, "The Super App Monopoly Probe in Southeast Asia," Hansaj Ekalavya, March 2024, available at: <https://hansajekalavya.com/super-app-monopoly-probe/>; Suy Se, "Revolution on the Road: The Rise of Ride Hailing Apps in Cambodia," Cambodianess, December 22, 2025, available at: <https://cambodianess.com/article/revolution-on-the-road-the-rise-of-ride-hailing-apps-in-cambodia>.

6 Inge Graef, "Market Definition and Market Power in Data: The Case of Online Platforms," World Competition 38 (2015): p. 477, available at: <https://doi.org/10.2139/ssrn.2657732>.



In turn, this raises the barrier to entry and reduces market competition, as it is difficult for new or even small competitors to compete effectively<sup>7</sup>. Moreover, these platforms may also engage in anti-competitive practices, such as predatory pricing, self-preferencing, or even the acquisition of smaller firms before they grow into potential competition<sup>8</sup>. These behaviors often stunt innovation and lead to concerns surrounding unfair competition practices and the ability of existing legal frameworks to effectively respond.

This brief argues that while Cambodia has already established general – albeit “light-touch” – regulatory frameworks to govern issues related to app-based mobility services, it has yet to be suitable and relevant in addressing the emergence of data-driven market power and network effects of dominant digital economies. Such challenges require proactive regulatory intervention, rather than a reliance on an ex-post, non-digital specific competition law regime. Against this backdrop, this paper places Cambodia’s Law on Competition (“**LOC**”) and other related regulatory frameworks under a magnifier, highlighting relevant problems, and offering recommendations to better address the abuse of dominance by digital platforms in app-based mobility services.

This paper is organized as follows: Section (I) introduces the legal problem; Section (II) analyzes existing laws and regulatory gaps; Section (III) proposes solutions, including the identification of digital dominance and the adoption of a multi-factor test; and Section (IV) concludes with key findings and recommendations.

## II. Reading Between the Gaps: Understanding Existing Laws & Regulatory Frameworks

### 1. Law on Competition

Article 9 of this law prohibits the abuse of a dominant market position where the conduct “significantly” prevents, restricts, or distorts competition<sup>9</sup>. This includes a non-exhaustive list of prohibited practices including: exclusive dealing, refusal to supply, tying arrangements, predatory pricing, and denial of competitors’ access to essential facilities. Notably, the law does not establish a quantitative threshold or criteria for the identification of a dominant market position. This lack of threshold, although it gives the regulating body flexibility, undermines legal certainty as it weakens the predictability for companies, and risks enforcement consistency – especially for digital markets, where factors used to determine dominance are difficult to measure.

Moreover, Cambodia’s flexible and principles-based approach allows for authorities – particularly the Cambodia Competition Commission (“**CCC**”<sup>10</sup>) to interpret and apply the law on a case-by-case basis. The CCC, alongside Cambodia’s competition regime is a relatively young regulatory body, thus, not only would there be a lack of historical dataset to accurately determine the numerical threshold, but the qualitative rules established from the case-by-case basis would further allow for the CCC to learn the Cambodian market behavior – albeit very gradually. While this flexibility may be beneficial in certain sectors of competition, in digital markets it poses serious enforceability challenges, since dominance is not reflected in market shares alone. Without proper quantitative thresholds, large platforms may potentially exploit this vagueness to justify their anti-competitive conduct.

Firstly, the law defines “dominant market position” as a situation in which a person has the power to act in a market significantly without any effective constraint from other competitors<sup>11</sup>. While this definition reflects a conventional competition law approach, it is not adequate to regulate digital platforms in app-based mobility services. For digital markets, the assessment of the degree of market power lies within a range of factors including data access, algorithms, network effects, multi-sidedness, and other features such as zero pricing, or non-price factors<sup>12</sup>.

Secondly, the legal language used in this provision is broad and vague – using terms like “significant” distortion of competition. Although the law defines “significantly prevent, restrict or distort” as the extent or degree of impact on competition for goods or services as determined by the CCC through economic analysis or any other means of analysis<sup>13</sup>, it still does not answer what metrics need to be used, nor does it define the threshold at which the conduct becomes unlawful. Additionally, the standard of this significant distortion is ex-post in nature, meaning that it is wholly dependent on proving harm that occurred after the fact, where

7 OECD, The Evolving Concept of Market Power in the Digital Economy, OECD Competition Policy Roundtable Background Note, DAF/COMP(2022)5 (Paris: OECD Publishing, 2022), p. 14, available at: <https://www.oecd.org/daf/competition/the-evolving-concept-of-market-power-in-the-digital-economy-2022.pdf>

8 *Ibid.*

9 Art. 9 of Law on Competition of Cambodia.

10 Art. 4 of Law on Competition of Cambodia Art. 1 and Art. 3 of Sub-Decree No. 37 on the Organization and Functioning of the Cambodia Competition Commission.

11 Art. 3(6) of Law on Competition of Cambodia.

12 OECD, Evolving Concept of Market Power, op. cit., 7.

13 Art. 3(14) of Law on Competition of Cambodia.

firms cannot easily determine whether their conduct would cross the prohibited threshold. It causes an over-reliance on the CCC's determination, risking legal uncertainty, unpredictability, and potential arbitrariness amongst firms.

Furthermore, Article 10 creates a justification for the undertakings of the prohibited conducts listed under its preceding provision if the CCC determines that there is "reasonable reason" for the business' benefits and demonstration that such conduct does not "significantly" harm competition<sup>14</sup>. Similarly, these terms are undefined and expansive. In digital markets, dominant platforms could just argue that practices such as dynamic or algorithmic pricing<sup>15</sup> and cross-market data leveraging<sup>16</sup> are efficiency enhancement practices that provide consumers with better products or lower prices. Thus, while Articles 9 and 10 effectively address the forms of abuse of dominance in traditional markets, they are not suited to capture the structural and data-driven nature of market power in digital platform markets.

Article 13 on the other hand, implies the ex-ante characteristic of the law, where parties involved in any agreements or activities that may prevent, restrict or distort competition, or constitute an abuse of dominant position, may request the CCC to review their actions before the performance of such an activity. In turn, the CCC could either reject the proposed agreements or activities if they are deemed in violation of Articles 7, 8, 9 or 11 of the law, or approve of the exemptions, subject to certain conditions.

## 2. Law on Electronic Commerce

As for the Law on Electronic Commerce ("LOEC"), although it does not substantively prohibit the abuse of dominance, it procedurally supports the LOC<sup>17</sup> by giving legal recognition to electronic<sup>18</sup> communications<sup>19</sup>, contracts<sup>20</sup>, and signatures<sup>21</sup>, and allows for the admissibility of electronic evidence as proof of abuse<sup>22</sup>. These articles allow for the regulating authorities or any affected parties to prove abusive conducts from dominant positions – such as unfair contract terms or exclusive contracts – by using app-based digital records.

Articles 30 regulates unsolicited commercial communications from businesses to consumers, providing the consumer with a clearly specified and easily activated option to reject such communications<sup>23</sup>. Large super apps often leverage their massive user databases to integrate various services into a single platform and push these new services onto users<sup>24</sup>. Although this article gives users the legal right to opt-out of these communications and in turn preventing a dominant platform from monopolizing their attention and digital space, it places the burden on the consumer to stop the spam; rather than requiring the digital platforms to obtain prior consent to opt-in. Moreover, this article only regulates unsolicited communication, it fails to regulate the dominant platforms' use of users' personal data to target those communications; allowing for access to user data such as ride history, to send "personalized" unsolicited offers or promotions that smaller platforms would not be able to match. Further, this law focuses only on more traditional communication methods like emails and do not explicitly regulate the algorithmic aspects of digital platforms such as suggesting recommendations on app-based mobility service platforms.

Lastly, Article 32 of this law imposes the obligation onto those handling electronic data to use "all means" to ensure that the data is protected by reasonable security safeguards to avoid loss, unauthorized access, usage, modification, leakage or disclosure<sup>25</sup>. It also prohibits interference with the electronic system to retrieve, copy, extract, delete or modify data in bad faith or without authorization<sup>26</sup>. While this article focuses on data security, it does not regulate data privacy such as how a digital platform can legitimately use, share or sell a user's data. This regulatory gap has direct implications for competition, as the control over data by dominant digital platforms without proper guidelines enables platforms to consolidate market power through network effects and conducts such as exclusionary practices, which raises the barrier to entry for competitors.

14 Art. 10 of Law on Competition of Cambodia.

15 M. Spann, M. Bertini, O. Koenigsberg et al., "Algorithmic Pricing: Implications for Marketing Strategy and Regulation," *International Journal of Research in Marketing* (2025), available at: <https://doi.org/10.1016/j.ijresmar.2025.05.001>.

16 Patrick F. Todd, "Digital Platforms and the Leverage Problem," *Nebraska Law Review* 98 (2020): p. 486, available at <https://digitalcommons.unl.edu/nlr/vol98/iss2/12>.

17 Art. 2(2) of Law on Electronic Commerce of Cambodia.

18 The terms "electronic" and "digital" are used synonymously in this brief.

19 Art. 5 of Law on Electronic Commerce of Cambodia.

20 Art. 12 of Law on Electronic Commerce of Cambodia.

21 Art. 7 of Law on Electronic Commerce of Cambodia.

22 Art. 11 and Art. 35 of Law on Electronic Commerce of Cambodia.

23 Art. 30 of Law on Electronic Commerce of Cambodia.

24 M. Hasselwander, "Digital Platforms' Growth Strategies and the Rise of Super Apps," *Heliyon* 10, no. 5 (2024): e25856, available at: <https://doi.org/10.1016/j.heliyon.2024.e25856>.

25 Art. 32(1) of Law on Electronic Commerce of Cambodia.

26 Art. 32(2) of Law on Electronic Commerce of Cambodia.

### III. Room for Recommendations: Best Practices for Implementation

#### 1. Introduction of Digital-Specific Guidelines on Dominance in Digital Markets

Articles 9 and 10 of the Law on Competition are fairly vague in their definition of dominant digital markets<sup>27</sup>. It could be that these provisions were intentionally left vague, to provide for flexibility and allow for adaptation over time. Given this broad language, the CCC should issue a formal and digital-specific guideline to clarify how dominance can be assessed under the Law on Competition. In particular, the guidelines should incorporate non-traditional indicators of market power, including network effects, data control, and platform dependency, which better reflect the structural realities of app-based mobility platforms. They should also offer practical examples of potentially abusive conduct, such as algorithmic pricing and self-preferencing, to illustrate how existing legal standards apply in data-driven environments.

In this regard, the European Union's ("EU") Digital Markets Act ("DMA"<sup>28</sup>) provides a useful comparative model, as it supplements traditional competition law by identifying key indicators of platform power, and through clarification of prohibited practices in digital markets. Cambodia does not need to replicate the DMA; however, adopting similar guidance would enhance legal certainty and predictability.

#### 2. The Adoption of a Multi-Factor Test for Digital Dominance

Although there are certain key players in the app-based mobility services sector in Southeast Asia, such as Grab<sup>29</sup>, there is yet to be a dominant player in Cambodia, as the market is fragmented with other major players including PassApp, WeGo, TADA, and LM Car<sup>30</sup>. Regardless, academics and policymakers have proposed adjustments in the way that authorities approach the determination of market power in digital markets<sup>31</sup>.

Market power or dominant position, is the ability of a firm to maintain prices above, or quality below a competitive level; and can make the difference between pro-competition and abusive firm conduct<sup>32</sup>. This is a similar concept to the definition laid out under Article 3(6) of the Cambodian Law on Competition, where dominant market position refers to a situation in which a person has the power to act in the market significantly without any effective constraint from other competitors<sup>33</sup>. The assessment of market power of more traditional sectors includes examining indicators such as market shares; however, market shares on their own have never been a complete proof of market power<sup>34</sup>. In digital markets, authorities such as the CCC should adopt a multi-factor test that elaborates on key digital indicators of digital dominance including network effects, data control, and algorithmic pricing – as these reflect the structural realities of app-based mobility markets.

#### A. Network Effects as Market Power in App-Based Mobility Services

Network effects apply to situations where the value of products or services increases as more users purchase the product or join the service<sup>35</sup>. For app-based mobility services, network effects are driven by both the increasing number of users that join to access the services, as well as the increasing number of drivers and vehicles available to provide such services<sup>36</sup>. What this essentially means is that an increase in the number of drivers lead to shorter waiting times, which leads to higher number of users (riders), leading to more drivers, creating a self-reinforcing feedback loop. Competition authorities could assess the network effects to determine the rate of users – both drivers and riders to determine dominance.

27 Art. 9–10 of Law on Electronic Commerce of Cambodia.

28 Digital Markets Act, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector, [2022] OJ L 265/1.

29 Zexiang Wang, "The Strategic Analysis of Grab's Strategic Dominance in Southeast Asia," *Journal of International Economy and Global Governance* 1, no. 3 (2024): pp.59–71, available at: <https://doi.org/10.12414/jiegg.240252>; Grab, "Grab Expansion Spells Confidence in Cambodia Rebound," November 23, 2021, <https://www.grab.com/kh/en/blog/grab-expansion-spells-confidence-in-cambodia-rebound-2/>.

30 Medeville, "Revolution on the Road," op. cit.; Rajni, "Top 6 Taxi Apps in Cambodia Offering Smart Travel Solutions," *Uber Taxi Clone Blog*, October 30, 2025, available at: <https://www.ubertaxiclone.com/blog/most-reliable-taxi-apps-in-cambodia/>.

31 OECD, *Evolving Concept of Market Power*, op. cit.

32 OECD, *Glossary of Statistical Terms* (n.d.), available at: <https://doi.org/10.1787/9789264055087-en>; OECD, *Abuse of Dominance in Digital Markets: Background Note by the Secretariat* (Paris: OECD Publishing, 2020), available at: <http://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf>.

33 Art. 3(6) of Law on Competition of Cambodia.

34 OECD, *Evolving Concept of Market Power*, op. cit.

35 Michael L. Katz and Carl Shapiro, "Network Externalities, Competition, and Compatibility," *American Economic Review* 75, no. 3 (1985): p.424.

36 Anna Woznica Hanusik, "Network Effects in Digital Transport Platform," *Communications of International Proceedings* (2024), available at: <https://doi.org/10.5171/2024.4430024>.

## B. Data Controllers, Where Data is Power

Large platforms' ability to continuously accumulate and combine its users' data allows for data control – which has emerged as a central source of market power in digital platform markets, particularly in app-based mobility services. Data control should be recognized as a key indicator of dominance in digital markets, as it constitutes a primary source of competitive advantage in platform-based business models. In app-based mobility services, platforms continuously collect and analyze large volumes of both user and operational data, allowing for optimized pricing, matching, and service delivery through algorithmic systems. This creates significant advantages that are difficult for competitors to replicate, thereby generating barriers to entry and reinforcing market power over time<sup>37</sup>. The accumulation of data further interacts with network effects, producing a self-reinforcing feedback loop in which increased user participation generates more data, improving service quality and attracting additional users. This results in a market power that is often structural and dynamic.

The DMA incorporates criteria such as user scale and platform intermediation power in identifying “gatekeepers,” implicitly acknowledging the role of data in entrenching dominance<sup>38</sup>. Particularly Article 3 of the DMA, which establishes the threshold based on user numbers and economic strength, while Articles 5 to 7 impose obligations addressing practices that may arise from data-driven advantages<sup>39</sup>.

## C. Pricing in the Digital Age

Algorithmic pricing has become a defining feature of digital platform markets, particularly in app-based mobility services, prices are dynamically determined through algorithmic systems that rely on real-time data inputs such as demand fluctuations, driver availability, geographic location, and user behavior.

While these systems can enhance efficiency by improving matching and reducing waiting times, they also raise significant competition concerns. In particular, algorithmic pricing allows platforms to exercise a high degree of control over market conditions, for example through price surging or personalized fare adjustments, which may facilitate exclusionary pricing strategies<sup>40</sup>. The opacity of these algorithms further complicates regulatory oversight, as pricing outcomes may appear competitive (such as lower fares for users) while masking underlying anti-competitive effects or unfair conditions imposed on drivers<sup>41</sup>.

Moreover, dominant app-based mobility platforms are able to leverage vast datasets on user demand and mobility patterns to continuously refine their pricing models, reinforcing their competitive advantage and creating barriers to entry for smaller competitors who lack access to comparable data<sup>42</sup>.

## 3. Strengthening Ex-Ante Regulatory Tools

Cambodia's competition law remains predominantly ex post, addressing anti-competitive conduct only after harm occurs. In digital platform markets this is inadequate as dominance can become entrenched rapidly through multi-sidedness, network effects, and massive data accumulation<sup>43</sup>. Moreover, especially in fast-moving digital markets, the pool of prior relevant cases is limited, from which precedents can be drawn from<sup>44</sup>. Thus, there is a growing shift toward a pre-emptive ex-ante regulatory approach, which prevents harm before it even occurs and detrimentally impacts competition and consumer welfare<sup>45</sup>, as these regulations would provide for clarity and increased certainty over what conducts are and are not acceptable. To combat this, it can be observed that the DMA targets structurally powerful “gatekeeper” platforms with its regulations<sup>46</sup>.

37 Annabelle Gawer and Carla Bonina, “Digital Platforms and Development: Risks to Competition and Their Regulatory Implications in Developing Countries,” *Information and Organization* 44 (2024): 100525, <https://www.sciencedirect.com/science/article/pii/S1471772724000253>.

38 Art. 3 of DMA, Regulation (EU) 2022/1925.

39 Art. 5–7 of DMA, Regulation (EU) 2022/1925.

40 Emilio Calvano, Giacomo Calzolari, Andrea Denicolò, and Sergio Pastorello, “Artificial Intelligence, Algorithmic Pricing, and Collusion,” *American Economic Review* 110, no. 10 (2020): pp. 3267–97.

41 OECD, *Algorithms and Collusion: Competition Policy in the Digital Age* (Paris: OECD Publishing, 2017).

42 Gawer and Bonina, “Digital Platforms and Development,” op. cit.

43 Philippe Libre, Ryan Jacido, Kimberly Diet, and Jessmond Elvina, *Managing Development of Digital Marketplaces in Asia*, chap. 7, Asian Development Bank, with comments and review by Johannes Benjamin Bernabe, James Villafuerte, and Josef T. Yap, available at: [https://aric.adb.org/pubs/digitalmarket/managing-development-digital-marketplaces-asia\\_CH7.pdf](https://aric.adb.org/pubs/digitalmarket/managing-development-digital-marketplaces-asia_CH7.pdf).

44 Competition and Markets Authority (CMA), *Online Platforms and Digital Advertising: Market Study Final Report* (London: CMA, 2020), available at: <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>.

45 Koki Arai, “Comparative Impacts of Ex Ante and Ex Post Regulation in Digital Markets: An Event Study Analysis of Stock Price Reactions,” *Asian Journal of Law and Economics* 16, no. 2 (2025): pp. 283–305, <https://doi.org/10.1515/ajle-2024-2002>.

46 Art. 3 and Art. 5–7 of DMA, Regulation (EU) 2022/1925.

Similarly, albeit more limited, Singapore's Competition and Consumer Commission has explored regulating "designated digital platforms" through obligations on transparency and fair dealings<sup>47</sup>. Reflecting a recognition that traditional ex-post tools are insufficient for digital markets.

#### 4. The Applicability of the DMA to the Cambodian Context

While the EU's DMA model provides for a useful reference in regulating dominant digital platforms, its relevance and applicability to Cambodia must be tailored to local market conditions. Cambodia's app-based mobility market remains dynamic and competitive, featuring multiple active major players operating alongside one another, without a single gatekeeper. Furthermore, the CCC is still developing its institutional capacity in the enforcement of antitrust laws. Therefore, rather than replicating the DMA's entire quantitative designation framework as a whole, Cambodia would benefit from strategically adopting targeted provisions. Specifically, the CCC would benefit from the underlying economic indicators of digital dominance that the DMA has established through platform dependency<sup>48</sup> and data control<sup>49</sup>.

#### IV. Conclusion

The rapid rise of app-based mobility services in Cambodia reflects broader transformations in urban transport systems driven by digitalization, platformization, and shifting consumer preferences. While these platforms deliver significant efficiencies and have become integral to mobility in cities such as Phnom Penh, they also introduce novel forms of market power that challenge the traditional competition law frameworks. As this brief has demonstrated, Cambodia's current regulatory regime (particularly under the Law on Competition) remains largely grounded in an ex-post, effects-based approach that is deficient in addressing the structural and data-driven nature of dominance in digital markets. The reliance on vague legal standards, the absence of clear criteria for identifying dominance, and the lack of digital-specific considerations limit the effectiveness of enforcement by the CCC.

In response, this paper has argued for a more adaptive and forward-looking approach. The introduction of digital-specific guidelines, the adoption of a multi-factor test incorporating network effects, data control, and algorithmic pricing, and the strengthening of ex ante regulatory tools would collectively enhance Cambodia's ability to identify and regulate dominant digital platforms. Comparative insights from the DMA and developments in Singapore further demonstrate that a shift toward preventive and structured regulation is both feasible and increasingly necessary.

Ultimately, Cambodia does not need to replace these models in full, but it must evolve beyond a purely reactive framework towards a proactive one. By integrating digital-specific indicators and adopting proportionate ex-ante regulations, Cambodia balance between fostering innovation and safeguarding competition. Such reforms would ensure that the benefits of app-based mobility services are preserved, while preventing the downsides of unchecked digital dominance in the long term.

---

47 Competition and Consumer Commission of Singapore (CCCS), Discussion Paper on Competition in Digital Markets (Singapore: CCCS, 2023).

48 Art. 2(2) and Art. 3 of DMA, Regulation (EU) 2022/1925.

49 Art. 5–6 of DMA, Regulation (EU) 2022/1925.



## Bibliography

### Laws and Regulations

1. Cambodia. Law on Competition. Royal Kram No. NS/RKM/1021/013. Promulgated October 5, 2021.
2. Cambodia. Law on Electronic Commerce. Royal Kram No. NS/RKM/1119/017. Promulgated November 2, 2019.
3. Cambodia. Sub Decree No. 37 ANKr.BK on the Organization and Functioning of the Cambodia Competition Commission. Promulgated February 17, 2022.
4. European Union. Digital Markets Act, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector. Official Journal of the European Union, L 265/1, 2022.

### Academic Journal Articles

1. Arai, Koki. "Comparative Impacts of Ex Ante and Ex Post Regulation in Digital Markets: An Event Study Analysis of Stock Price Reactions." *Asian Journal of Law and Economics* 16, no. 2 (2025): 283–305. <https://doi.org/10.1515/ajle-2024-2002>.
2. Calvano, Emilio, Giacomo Calzolari, Andrea Denicolò, and Sergio Pastorello. "Artificial Intelligence, Algorithmic Pricing, and Collusion." *American Economic Review* 110, no. 10 (2020): 3267–3297.
3. Chalermpong, Saksith, Hironori Kato, Phathinan Thaihatkul, Apiwat Ratanawaraha, Alexis Fillone, Nguyen Hoang Tung, and Peraphan Jittrapirom. "Ride hailing applications in Southeast Asia: A literature review." *International Journal of Sustainable Transportation*, 2022. <https://doi.org/10.1080/15568318.2022.2032885>
4. Gawer, Annabelle, and Carla Bonina. "Digital Platforms and Development: Risks to Competition and Their Regulatory Implications in Developing Countries." *Information and Organization* 44 (2024): 100525. <https://www.sciencedirect.com/science/article/pii/S1471772724000253>.
5. Graef, Inge. "Market Definition and Market Power in Data: The Case of Online Platforms." *World Competition* 38 (2015): 473–505. <https://doi.org/10.2139/ssrn.2657732>
6. Hasselwander, M. "Digital Platforms' Growth Strategies and the Rise of Super Apps." *Heliyon* 10, no. 5 (2024): e25856. <https://doi.org/10.1016/j.heliyon.2024.e25856>.
7. Katz, Michael L., and Carl Shapiro. "Network Externalities, Competition, and Compatibility." *American Economic Review* 75, no. 3 (1985): 424–440.
8. Spann, M., Bertini, M., Koenigsberg, O., et al. "Algorithmic Pricing: Implications for Marketing Strategy and Regulation." *International Journal of Research in Marketing*. 2025. <https://doi.org/10.1016/j.ijresmar.2025.05.001>.
9. Todd, Patrick F. "Digital Platforms and the Leverage Problem." *Nebraska Law Review* 98 (2020): 486. Available at <https://digitalcommons.unl.edu/nlr/vol98/iss2/12>.
10. Wang, Zexiang. "The Strategic Analysis of Grab's Strategic Dominance in Southeast Asia." *Journal of International Economy and Global Governance* 1, no. 3 (2024): 59–71. <https://doi.org/10.12414/jiegg.240252>.
11. Woznica Hanusik, Anna. "Network Effects in Digital Transport Platform." *Communications of International Proceedings*. 2024. <https://doi.org/10.5171/2024.4430024>.

### Institutional Reports

1. Competition and Consumer Commission of Singapore (CCCS). Discussion Paper on Competition in Digital Markets. Singapore: CCCS, 2023.
2. Competition and Markets Authority (CMA). Online Platforms and Digital Advertising: Market Study Final Report. London: CMA, 2020. <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>.
3. International Transport Forum (ITF). Regulating app based mobility: Case Studies from Bangkok, Manila, and Phnom Penh. International Transport Forum Policy Papers, No. 139. Paris: OECD Publishing, 2024.
4. Libre, Philippe, Ryan Jacildo, Kimberly Diet, and Jessmond Elvina. Managing Development of Digital Marketplaces in Asia. Chap. 7. Asian Development Bank. With comments and review by Johannes Benjamin Bernabe, James Villafuerte, and Josef T. Yap. [https://aric.adb.org/pubs/digitalmarket/managing-development-digital-marketplaces-asia\\_CH7.pdf](https://aric.adb.org/pubs/digitalmarket/managing-development-digital-marketplaces-asia_CH7.pdf).
5. OECD. Abuse of Dominance in Digital Markets: Background Note by the Secretariat. Paris: OECD Publishing, 2020. <http://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf>.
6. OECD. Algorithms and Collusion: Competition Policy in the Digital Age. Paris: OECD Publishing, 2017.
7. OECD. Glossary of Statistical Terms (n.d.), available at: <https://doi.org/10.1787/9789264055087-en>.
8. OECD. The Evolving Concept of Market Power in the Digital Economy. OECD Competition Policy Round-

## News Articles, Blogs & Commentaries

1. Grab. "Grab Expansion Spells Confidence in Cambodia Rebound." November 23, 2021. <https://www.grab.com/kh/en/blog/grab-expansion-spells-confidence-in-cambodia-rebound-2/>.
2. Hansaj, Ekalavya. "The Super App Monopoly Probe in Southeast Asia." Hansaj Ekalavya. March 2024. <https://hansajekalavya.com/super-app-monopoly-probe/>.
3. Medeville, Pascal. "Revolution on the Road: The Rise of Ride Hailing Apps in Cambodia." Wonders of Cambodia. February 23, 2026. <https://wondersofcambodia.com/revolution-on-the-road-the-rise-of-ride-hailing-apps-in-cambodia/>.
4. Rajni. "Top 6 Taxi Apps in Cambodia Offering Smart Travel Solutions." Uber Taxi Clone Blog. October 30, 2025. <https://www.ubertaxiclone.com/blog/most-reliable-taxi-apps-in-cambodia/>.
5. Se, Suy. "Revolution on the Road: The Rise of Ride Hailing Apps in Cambodia." Cambodianess. December 22, 2025. <https://cambodianess.com/article/revolution-on-the-road-the-rise-of-ride-hailing-apps-in-cambodia>.

## Data Sources

1. World Bank. "Mobile cellular subscriptions (per 100 people)." World Development Indicators. <https://data.worldbank.org/indicator/IT.CEL.SETS.P2>.



**Conditionality in The Formation of Electronic  
Contracts:  
Does It Ensure a Fair and Balanced Relationship between Parties?**

*HORN Sokngim*

## Abstract

The rise of electronic contracting has replaced negotiated agreements with standardised, non-negotiable digital terms, raising the question of whether the conditionality embedded in click-wrap, browse-wrap, and automated-system contracts is compatible with genuine consent and a fair balance of contractual power. As consumer transactions migrate almost entirely onto electronic commerce (“e-commerce”) platforms, mobile applications, and automated payment and subscription systems, the classical model of contract, an offer met by a deliberated, negotiated acceptance, has given way to a binary act of clicking “I agree” to terms drafted unilaterally by the business operator. This shift raises a foundational tension in contract law. Consent has traditionally been regarded as evidence of a fair bargain. Yet, when contractual terms are non-negotiable, rarely read, and can be changed unilaterally by the drafter, clicking “I agree” may no longer represent genuine agreement or a fair allocation of rights and risk.

This brief examines that question under Cambodian law by analysing the Civil Code (2007), the Law on Electronic Commerce (2019), the Law on Consumer Protection (2019), and Prakas No. 0067 on Unfair Contract Clauses (2022). It finds that while these instruments secure the formal validity and enforceability of electronic contracts, they regulate the procedural conditions of contract formation more thoroughly than the substantive fairness of the terms imposed, leaving consumers exposed to unilateral modification clauses, bundled data-processing conditions, and manipulative interface design. Drawing a comparative lens from the European Union’s Unfair Contract Terms Directive, the General Data Protection Regulation, and the Digital Services Act, this brief argues that formal consent should not be equated with contractual fairness. It concludes with policy recommendations for Cambodia, including a definitive list of automatically void unfair digital terms, simplified disclosure of material contractual conditions, explicit regulation of dark patterns, and accessible dispute resolution mechanisms for digital consumers, so that Cambodia’s legal framework evolves from merely validating electronic agreements to ensuring their substantive fairness.

## I. Introduction

The rapid growth of the digital economy has revolutionized the manner in which contracts are formed and performed<sup>1</sup>. This rapid transformation has shifted conventional contract practices into digital forms known as electronic contracts (“e-contracts”) concluded through digital interfaces such as online platforms, mobile applications, and automated systems<sup>2</sup>. Consumers now routinely enter into e-contracts when accessing online platforms, purchasing digital goods, subscribing to services, or creating accounts such as social media or e-commerce websites. Unlike traditional contracts, e-contracts are commonly concluded through automated systems and standard-form agreements that require users to accept pre-drafted standardized terms and conditions that presented on a non-negotiable, “take-it-or-leave-it” basis, where users express consent by clicking an “I Agree” button or taking a similar electronic action<sup>3</sup>. Consequently, contractual relationships are increasingly formed without any genuine negotiation between the parties, giving rise to a structural risk of imbalance in bargaining power<sup>4</sup>.

In Cambodia, this development has been addressed through the Law on Electronic Commerce (“LEC”) in 2019, which recognises the legal validity of electronic communications, electronic signatures, and automated contract formation. In particular, the law confirms that electronic contracts cannot be denied validity solely on the basis of their electronic form and allows legal requirements relating to writing and signatures to be satisfied digitally. While these provisions ensure legal certainty, they primarily address the formal validity of electronic contracts rather than their substantive fairness. As a result, significant concerns remain regarding whether electronic contracts, particularly those based on standardised and non-negotiable terms, adequately reflect genuine consent and maintain a fair balance between contracting parties. In practice, consumers have limited ability to negotiate, modify, or reject contractual terms, particularly where access to essential digital services is conditional upon acceptance. The central legal question this brief examines is whether such conditionality ensures a fair and balanced relationship between contracting parties, or whether it merely reinforces structural imbalances under the guise of technological efficiency. This brief primarily examines conditionality under laws of the Kingdom of Cambodia (“Cambodia”) and further draws upon the comparative standards of the European Union to identify the current limitations of the Cambodian framework and to

1 Duaa Hijazi et al., “Electronic Commercial Contracts in Saudi Arabia: Legal and Regulatory Challenges,” *International Journal of Innovative Science and Research Technology* 9, no. 9 (2024): pp. 2214–2221.

2 P. A. N. Kasim, “Good Faith in Electronic Contracts and Online Consumer Protection: A Normative Study,” *Progressive Law Review* 6, no. 1 (2024).

3 Robert A. Hillman and Jeffrey J. Rachlinski, “Standard-Form Contracting in the Electronic Age,” *New York University Law Review* 77, no. 2 (2002): 429, 436.

4 Friedrich Kessler, “Contracts of Adhesion—Some Thoughts About Freedom of Contract,” *Columbia Law Review* 43, no. 5 (1943): 629–42.

propose concrete pathways for reform.

## II. The Legal Framework of Electronic Contracts Under the Law of Cambodia

To assess the impact of digital conditionality, it is important to first understand the legal framework governing contract formation in Cambodia. Electronic contracts in Cambodia are governed by both traditional principles of contract law and modern laws regulating electronic transactions. These rules provide the legal basis for the formation, recognition, and enforcement of contracts concluded through electronic means.

The Civil Code of Cambodia (“**Civil Code**”) (2007) remains the primary source of general contractual obligations. Under Article 336 of the Civil Code, a legally binding contract is formed once an offer and the acceptance thereto conform to each other<sup>5</sup>. The Civil Code presupposes that both parties have the freedom and ability to consider the contractual terms, to understand their rights and obligations, and to express genuine consent free from defects such as fraud, misrepresentation, or duress<sup>6</sup>. This approach reflects the traditional understanding of contract formation, which is founded on mutual agreement and informed consent between both parties.

As commerce progressively migrated to online platforms, the Cambodian legislature recognized the need to extend formal legal validity to digital transactions, culminating in the enactment of the Law on Electronic Commerce (2019) (“**LEC**”). Article 12 of LEC explicitly grants legal recognition, validity, and enforceability to offers, acceptances, and expressions of intent communicated through electronic means, and establishes that a contract shall not be denied legal effect solely on the basis that it was concluded in electronic form<sup>7</sup>. This provision was essential in removing legal uncertainty surrounding paperless transactions and giving the public confidence in the use of electronic communication<sup>8</sup>.

However, Article 16 of LEC creates a significant structural complication. It states that a proposal to enter into a contract through an electronic communication that is not addressed to a specific person is considered as an invitation to make an offer<sup>9</sup>. The law uses the phrase ‘an invitation’ rather than a binding offer in itself. It only becomes a binding offer if the platform clearly shows an intention to be bound upon acceptance<sup>10</sup>. Digital platforms exploit this statutory distinction by designing conditional systems that place the user in the position of the offeror, whose offer is pre-drafted to incorporate the platform’s extensive and non-negotiable terms of service in their entirety<sup>11</sup>. This structure shifts away from the traditional model of mutual negotiation under the Civil Code and effectively shifts the entire burden of contractual risk onto the user from the outset.

## III. Automated Systems, Conditions Precedent, And the Problem of Genuine Consent

The problem of unequal bargaining power intensifies when contracts move beyond manual click-wrap interfaces to fully automated systems. Article 17 of the LEC expressly recognizes the contracts formed through the interaction of a person with an automated electronic system, such as pre-programmed application algorithms, artificial intelligence engines, or smart contract protocols, establishing that such contracts shall not be denied validity or enforceability on the ground that no natural person directly reviewed or intervened in their formation<sup>12</sup>. While this provision is commercially necessary to facilitate modern digital commerce, it also carries a legal risk. In practice, it enables contracts to be formed instantly and without negotiation on a broad scale, which may strengthen the use of pre-drafted and non-negotiated conditions in digital transactions.

Where an algorithm triggers a conditional clause, such as one that automatically triggers a contractual condition, for example, by deducting a payment, transferring data rights, or terminating a user’s access to a digital asset upon the occurrence of a specified event, the consumer is bound immediately and without warning. The Law does provide a limited right of correction where a natural person makes an input error in

5 Civil Code of Cambodia, Royal Kram No. NS/RKM/1207/030 (8 December 2007), Art. 336.

6 DFDL, “The Implementation of Cambodia’s New Civil Code,” DFDL, September 15, 2023, <https://www.dfdl.com/insights/legal-and-tax-updates/the-implementation-of-cambodias-new-civil-code-2/>

7 Law on Electronic Commerce of Cambodia, Royal Kram No. NS/RKM/1119/017 (2 November 2019), Art. 12.

8 Law on Electronic Commerce of Cambodia, op. cit., Art. 1; Tilleke & Gibbins, “Cambodia Enacts a New E-commerce Law and a Consumer Protection Law,” Tilleke & Gibbins, December 10, 2020, <https://www.tilleke.com/insights/cambodia-enacts-new-e-commerce-law-and-consumer-protection-law/>

9 Law on Electronic Commerce of Cambodia, op. cit., Art.16.

10 Law on Electronic Commerce of Cambodia, op. cit., Art.16.

11 Nop Legal, “Oral or Verbal Employment Contract in Cambodia,” Nop Legal, July 22, 2021, <https://noplegal.com/2021/07/22/oral-or-verbal-employment-contract-in-cambodia/>

12 Law on Electronic Commerce of Cambodia, op. cit., Art. 17.



an automated electronic communication that fails to offer an opportunity to correct it<sup>13</sup>, but this protection applies only to input errors, not to the broader problem of a consumer being bound by conditions they never genuinely and meaningfully understood.

This reality gives rise to what may be described as the “consent myth” in digital commerce, whereby compliance with the formal conditions required for electronic contract formation is treated as equivalent to meaningful contractual consent, despite the absence of genuine understanding or bargaining power. The user performs the acts that satisfy the technical formalities of assent under Article 5 of LEC yet lacks the genuine comprehension of what the automated conditions embedded in the platform’s code will do once triggered. Furthermore, conditions precedent in digital contracts, conditions that must be satisfied before a user’s rights take effect or before a platform’s obligations activate, are frequently used not to allocate risk between the parties, but to impose unilateral control. For example, a platform may include a condition that voids a user’s right to a refund after a single use of a service, or one that automatically suspends account access based on algorithmic detection of a possible violation of a broadly defined acceptable use policy, without human review.

The absence of meaningful negotiation, the extreme length and technical complexity of standard digital terms of service, and the structural pressure of “take-it-or-leave-it” choices collectively prevent genuine consent from being formed. Until Cambodian courts develop a substantial body of case law specifically scrutinizing automated digital conditions, consumers remain largely unprotected against terms they never genuinely agreed to.

#### **IV. Bargaining Power Asymmetry and the Limits of Consumer Protection Law**

The contractual imbalance inherent in digital conditionality is at its most pronounced in the context of contracts of adhesion. These are the standard-form contracts drafted exclusively by the stronger party and offered to consumers on a strict “take-it-or-leave-it” basis. In such cases, the consumer has no real ability to counter, negotiate, amend, or remove unfair terms. This model now dominates digital service agreements, software licences, platform terms of use, and online marketplace contracts<sup>14</sup>.

In Cambodia, the Law on Consumer Protection (“LCP”) (2019) is the main legal instrument addressing this imbalance. For instance, Chapters 4 and 5 of the LCP explicitly prohibit unfair trading practices and deceptive commercial conduct<sup>15</sup>. Chapter 6 of LEC further imposes mandatory information disclosure obligations on electronic commerce operators, requiring them to provide clear, accurate, and accessible information regarding the products, prices, and contract terms<sup>16</sup>. More specifically, Prakas No. 0067 on Unfair Contract Clause, issued by the Ministry of Commerce on 1 March 2022 pursuant to the Law on Consumer Protection, provides the most direct regulatory response to contractual imbalance in standard-form contracts<sup>17</sup>. This Prakas applies to all standard-form contracts pre-formulated by business operators for the provision of goods and/or services to consumers, where consumers have no opportunity to negotiate or modify the terms in any form<sup>18</sup>. It prohibits contractual clauses that confer excessive benefits to the business operator or that create unfair and unjustified disadvantage to consumers in a manner that exploits the consumer’s economic difficulties, ignorance, or inexperience<sup>19</sup>. Any use of such a clause is deemed an unfair act and unfair practice under the Law on Consumer Protection, and may result in administrative penalties, including fines of up to KHR 50,000,000 (approximately USD 12,500<sup>20</sup>).

Despite these legal protections, a critical gap remains in the enforcement regime. The current rules mainly focus on procedure rather than substance. They require businesses to disclose information and make terms accessible, but they do not directly control whether the terms themselves are fair. As a result, a digital service provider in Cambodia may fully comply with the law by clearly publishing its terms of use, while still including clauses that allow it to change services unilaterally, increase fees without notice, or fully exclude liability for service failures. In practice, such disclosure alone does not remove unfairness in the contract terms. Consumers often accept these terms due to economic necessity or lack of alternatives. This means that procedural compliance can create an appearance of fairness, even where the actual contractual terms remain highly imbalanced and potentially exploitative. In addition, Cambodia still lacks comprehensive data

13 Law on Electronic Commerce of Cambodia, op. cit., Art. 18.

14 Rafał Mańko, “Unfair Contract Terms in EU Law: Unfair Terms Directive and Common European Sales Law,” European Parliamentary Research Service (Brussels: European Parliament, 2013), p.1.

15 Law on Consumer Protection of Cambodia, Royal Kram No. NS/RKM/1119/016 (2 November 2019), Chs. 4–5.

16 Law on Electronic Commerce of Cambodia, op. cit., Ch. 6.

17 Prakas No. 0067 P.N.A.KBB.PRK on Unfair Contract Clause (1 March 2022).

18 DFDL, “Cambodia: Implementation of Prakas on Unfair Contract Terms,” DFDL, February 7, 2024, <https://www.dfdl.com/insights/legal-and-tax-updates/cambodia-implementation-of-prakas-on-unfair-contract-terms/>

19 Prakas No. 0067 P.N.A.KBB.PRK on Unfair Contract Clause, op. cit.

20 Siphana & Associates, “Prakas on Unfair Contractual Terms Issued to Enhance Consumer Protection,” Siphana & Associates, July 4, 2023, <https://www.soksiphana.com/resources/alerts/ministerial-prakas-on-unfair-contractual-terms-issued-to-enhance-consumer-protection/>

protection legislation, despite the publication of a draft Law on Personal Data Protection in July 2023<sup>21</sup>. Until this law is enacted, data-related conditionality, requiring users to accept extensive data collection and sharing as a condition of access, remains largely unregulated, leaving consumers without a specific legal remedy.

Accordingly, although Cambodian law regulates the procedural conditions under which electronic contracts are formed, it provides only limited scrutiny of the substantive conditions imposed upon consumers. This allows digital conditionality to function as a mechanism for enforcing contractual imbalance, notwithstanding formal compliance with the legal requirements for electronic contract formation.

## V. Comparative Analysis: Substantive Remedies Under European Union Law

To bridge the gap between formal procedural compliance and genuine contractual fairness, Cambodia's evolving legal framework may usefully draw upon the comparative standards of the European Union ("EU"). Unlike legal regimes that focus primarily on disclosure and procedural validity, EU law increasingly regulates the substantive fairness of contractual terms and the digital practices through which consumer consent is obtained.

The cornerstone of this framework is the Unfair Contract Terms Directive ("UCTD"). Article 3(1) provides that a contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer<sup>22</sup>. Under the UCTD, the mere fact that a consumer has formally accepted a contractual term does not preclude judicial scrutiny of its fairness. To eliminate ambiguity in the application of this standard, the UCTD includes an Annex containing a non-exhaustive indicative list, commonly described in legal commentary as the "grey list", of terms that may be regarded as unfair<sup>23</sup>. These include clauses granting the trader the unilateral right to alter the terms of the contract without a valid, pre-defined reason specified in the contract; provisions permitting the seller to retain sums paid by the consumer where the consumer decides not to conclude or perform the contract without providing the consumer with an equivalent right to compensation; and terms that irrevocably bind the consumer to conditions which the consumer had no real opportunity to become acquainted with before conclusion of the contract<sup>24</sup>. In many Member States, national implementing legislation further provides that particularly abusive terms are automatically void and unenforceable, regardless of whether the consumer was technically informed of their existence.

The EU has subsequently supplemented this framework through legislation specifically addressing digital transactions and data-driven business models. The General Data Protection Regulation ("GDPR") introduces the concept of freely given, specific, informed, and unambiguous consent. Article 7(4), read together with Recital 43, provides that consent should not be regarded as freely given where there is a clear imbalance between the parties, particularly where consent to the processing of personal data is bundled as a non-negotiable condition for the provision of a service<sup>25</sup>. The European Data Protection Board has further clarified that where consent is bundled as a non-negotiable component of terms and conditions, it is presumed not to have been freely given<sup>26</sup>.

The Digital Services Act ("DSA") further extends consumer protection into the design of digital interfaces. Article 25(1) prohibits online platforms from designing, organizing, or operating online interfaces in a manner that deceives, manipulates, or materially distorts users' ability to make free and informed decisions<sup>27</sup>. Recital 67 specifically identifies so-called "dark patterns"—interface designs that undermine or impair user autonomy—as falling within the scope of this prohibition<sup>28</sup>. This is the first EU instrument to expressly name dark patterns as a prohibited practice in primary legislation<sup>29</sup>.

21 Graham Greenleaf, "Cambodia's Draft Data Privacy Law: Too Much is Left to Delegated Prakas", SSRN Working Paper (2025), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5206970](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5206970); Hogan Lovells, "Cambodia Moves to Enact Comprehensive Data Privacy Law" (July 2025).

22 Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts (1993) OJ L 95/29, Art. 3(1).

23 Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts, op. cit., Annex.

24 European Commission, "Unfair Contract Terms Directive," European Commission, updated 2022, [https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/unfair-contract-terms-directive\\_en](https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/unfair-contract-terms-directive_en)

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L 119/1, Art. 7(4) and Recital 43.

26 European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 (Version 1.1, adopted 4 May 2020), p. 6, available at: [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf)

27 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L 277/1, Art. 25(1).

28 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), op. cit., Art. 25(1) and Recital 67.

29 Mason Hayes & Curran, "Transparency Under the EU Digital Services Act," Mason Hayes & Curran, updated December 2025, <https://www.mhc.ie/latest/insights/transparency-under-the-eu-digital-services-act>

The comparative significance of the EU framework lies in its recognition that formal consent alone is insufficient to guarantee contractual fairness. Rather than relying exclusively on disclosure obligations, EU law addresses imbalance at multiple levels: the substantive content of contractual terms, the conditions under which consent is obtained, and the design of digital interfaces that influence consumer decision-making. By contrast, Cambodian law remains primarily focused on ensuring the validity and enforceability of electronic transactions. Although Prakas No. 0067 and the Consumer Protection Law represent important developments in protecting consumers against unfair practices, they do not yet provide detailed categories of prohibited contractual terms, automatic mechanisms for invalidating manifestly unfair provisions, or explicit regulation of manipulative digital design practices<sup>30</sup>.

The EU experience suggests that greater legal certainty could be achieved through the adoption of more specific statutory rules identifying unfair digital contractual practices and establishing clearer consequences for non-compliance. Such reforms would strengthen the practical protection of consumers while preserving the efficiency and legal certainty necessary for the continued growth of electronic commerce in the digital environment<sup>31</sup>.

## VI. Recommendations

To strengthen consumer protection while preserving commercial certainty and digital innovation, the following reforms merit consideration. First, the Ministry of Commerce should consider adopting a definitive list of prohibited digital contract terms that are automatically null and unenforceable, regardless of disclosure or consumer acceptance. Such terms may include unilateral modification clauses without objectively justified reasons, blanket exclusions of liability for essential service failures, and contractual provisions that unreasonably restrict access to judicial remedies. Second, legislation should require simplified and standardized disclosure of key contractual conditions before consumers provide electronic consent. Material provisions relating to automatic renewal, data-sharing practices, limitations of liability, and dispute resolution mechanisms should be presented in a clear, concise, and easily accessible format rather than being embedded within lengthy terms of service. Third, Cambodia should consider introducing explicit regulation of manipulative digital interface practices, including so-called “dark patterns”, that impair consumers’ ability to make free and informed decisions. Prohibiting deceptive interface design would complement existing protections against unfair commercial practices and strengthen the integrity of electronic consent. Fourth, establishment of an accessible and low-cost dispute resolution mechanism for digital consumer disputes would significantly enhance the practical enforceability of existing legal protections. Effective consumer rights depend not only on substantive legal standards but also on realistic avenues for redress.

## VII. Conclusion

The foregoing analysis leads to the conclusion that the current paradigm of conditionality in the formation of electronic contracts does not inherently ensure a fair or balanced relationship between contracting parties. Instead, it functions as a highly efficient legal mechanism through which corporate entities formalize and enforce structural advantages over users who have no realistic ability to negotiate, contest, or refuse the conditions imposed upon them. Cambodia’s legislative framework, comprising the Civil Code, LEC, LCP, and Prakas No. 0067, provides a sound foundation for the recognition and enforcement of electronic contracts. These instruments collectively ensure the validity of electronic consent and establish general safeguards against unfair contractual practices. However, the framework remains primarily focused on the procedural validity of contract formation rather than addressing the structural inequalities that characterize many contemporary digital transactions. In practice, electronic contracts are frequently concluded through standardized and non-negotiable acceptance mechanisms that offer consumers little or no meaningful opportunity to influence contractual terms. The widespread use of click-wrap agreements, bundled data-processing conditions, and platform-designed interfaces may therefore produce a significant imbalance in bargaining power despite the formal existence of consent. Consequently, legal validity should not be equated with contractual fairness. Comparative analysis of the European Union framework illustrates that modern consumer protection increasingly extends beyond disclosure requirements to address the substantive fairness of contractual terms, the conditions under which consent is obtained, and the design of digital interfaces that influence consumer decision-making. These developments offer useful guidance for the continued evolution of Cambodian law. Ultimately, the challenge facing Cambodian law is not whether electronic contracts should be recognized—they already are—but whether the conditions under which they are formed adequately protect

30 Pinsent Masons, “Dark Patterns Case Sees Digital Regulation and Consumer Law,” Pinsent Masons, October 2025, <https://www.pinsentmasons.com/out-law/analysis/dark-patterns-digital-regulation-consumer-law>

31 “Policing Consumer Contract Terms under US and EU Law: A Comparative Analysis of Directive 93/13/EEC and the Restatement of Consumer Contracts,” German Law Journal (2025), <https://www.cambridge.org/core/journals/german-law-journal/article/policing-consumer-contract-terms-under-us-and-eu-law-a-comparative-analysis-of-the-directive-9313eec-on-unfair-terms-in-consumer-contracts-and-the-restatement-of-consumer-contracts/78EF06068AC89F7DBBEF03A95198B4F4>

the principles of fairness, good faith, and meaningful consent. As digital transactions continue to permeate everyday economic life, the law must evolve beyond validating electronic agreements and toward ensuring that the benefits of digital commerce are accompanied by an appropriate level of substantive consumer protection. Only then can conditionality in electronic contracting operate as a mechanism of both commercial efficiency and contractual justice.





## PART II CRIMINAL PROCEDURES IN THE CONTEXT OF CYBERCRIME





## **Digital Evidence Acquisition from Smartphones and Computers in Cambodian Criminal Proceedings**

*SOMNANG Odom*

## Abstract

On 31 March 2026, the Ministry of Interior of the Kingdom of Cambodia ('MOI') and Korea International Co-operation Agency ('KOICA') signed a USD 13.5 million agreement to upgrade the digital forensic laboratories at the General Commissariat of National Police ('GCNP'<sup>1</sup>); however, in the absence of clear provisions in the Code of Criminal Procedure (2007) ('CCP'), it affects the lawful acquisition of digital evidence seized from digital devices such as smartphones or computers. Articles 92 and 160 of the CCP require judicial police officers and investigating judges to affix a physical seal to seized exhibits, which cannot be adapted to the context of digital data. Furthermore, Article 109 of the CCP enumerates Article 92 among the mandatory rules whose violation renders the resulting evidence null and void in flagrant offence inquiries, while Article 252 imposes a parallel mandatory-rule regime in judicial investigations and captures Article 160 through its comprehensive clause for 'any substantial rule or procedure' affecting the interests of the concerned party. However, Articles 91 and 159 of the CCP were drafted primarily with physical searches and the seizure of tangible evidence in mind, without incorporating procedural safeguards tailored to the distinctive characteristics of digital evidence, including its volatility, susceptibility to alteration, and the technical requirements for forensic acquisition and integrity preservation. Lastly, Article 321 mirrors the doctrine of intime conviction enshrined in Article 427 of the French Code de procédure pénale (2025) ('FCPP'), which provided:

*'Except where the law otherwise provides, offences may be proved by any mode of evidence and the judge decides according to his innermost conviction.'*

This confers broad judicial discretion in assessing the probative value of evidence in the absence of specific authentication standards or objective criteria and provides no objective technical threshold for evaluating digitally acquired evidence. This legal brief argues that the resulting systemic gap should be closed through a proposed Sub-Decree on Collection, Acquisition, Preservation, and Presentation of Digital Evidence grounded in five principles: authorisation, non-alteration, integrity verification, documentation, and proportionality, adapted from ISO/IEC 27037 (2012) ('ISO/IEC'), Singapore's Criminal Procedure Code (2010) ('SCPC'), FCPP, and recent jurisprudence.

## I. Introduction

On 31 March 2026, MOI and KOICA signed a USD 13.5 million agreement to upgrade digital forensic facilities at the GCNP and establish a state-of-the-art forensic science laboratory at the Police Academy<sup>2</sup>. The procedural legal framework governing digital evidence acquisition, however, has not kept pace with these developments. Digitalisation has transformed criminal activity in two analytically distinct ways. First, digital technologies have scaled and accelerated traditional crimes such as fraud and money laundering through organised black markets and networked criminal infrastructure<sup>3</sup>. Second, new categories of offences have emerged that are native to the digital environment, including online scams, identity theft, unauthorised access, and information technology-based fraud of the kind now addressed by Cambodia's Law on Combating Online Scams (2026) ('LCO'<sup>4</sup>). A growing subset of this second category comprises cyber-enabled offences such as cyberattacks, ransomware, and online fraud, which extend rather than displace the offences already described and which generate evidentiary traces primarily in digital form. As Casey explains, the role of computers in crime determines how they function as evidence, and where they play a central role, they often constitute key evidentiary sources<sup>5</sup>. Moreover, digital evidence may be as significant as physical evidence in both criminal and civil proceedings, particularly in reconstructing events and identifying offenders<sup>6</sup>. This is reflected in law enforcement practice, where there is a 'continuous trend towards investigations relying on some form of digital evidence'<sup>7</sup>.

1 'Forensic Investigation Capacity Gets \$13.5 Million Boost,' Khmer Times, 1 April 2026, <https://www.khmertimeskh.com/501872247/forensic-investigation-capacity-gets-13-5-million-boost/>.

2 Khmer Times, 'Forensic Investigation Capacity Gets \$13.5 Million Boost,' op. cit.

3 UNODC, 'Comprehensive Study of the Problem of Cybercrime and Responses to It by Member States, the International Community and the Private Sector,' Expert Group Report, UNODC/CCPCJ/EG.4/2013/2 (January 23, 2013), 3.

4 Kingdom of Cambodia, Law on Combating Online Scams (2026).

5 Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Waltham, MA: Academic Press, 2011), 39, ch. 2, §2.2, 'The Role of Computers in Crime,' para. 2; see also 41, para. 2, discussing computers as sources of digital evidence.

6 Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, 3rd ed. (Abingdon, Oxon: Routledge, 2022), 555–557, ch. 14, 'Evolution of Digital Forensics,' section 'The Role of Digital Evidence,' discussing digital evidence's role in linking victims, offenders, places, and objects, reconstructing events, identifying suspects, and its importance in criminal and civil cases.

7 INTERPOL, Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence (Lyon: INTERPOL General Secretariat, 2021), 5 (Foreword, para. 2).

Cambodia is no exception: a report drawing on a United Nations Office on Drugs and Crime ('UNODC') map describes the country as a host to multiple scam hubs and as a global centre for such operations<sup>8</sup>.

## II. A Law Written for Physical Evidence

The CCP addressed searches and seizures through two parallel tracks. Articles 19 and 92 govern flagrant offence investigation, conducted by judicial police officers under prosecutorial authorisation. Articles 159 and 160 of the CCP govern judicial investigation, conducted by or under the authority of an investigating judge. Article 321 governs evidentiary evaluation by the court. None of these provisions anticipates the acquisition of data from inside a seized digital device<sup>9</sup>. Articles 92 and 160 of the CCP are the provisions most directly relevant to this very brief, as both Articles govern what an authorised authority must do with a seized exhibit. Both require a physical seal and a written confiscation record. A physical seal certifies that the object has not been tampered with, but it cannot certify whether the digital data inside the object was altered while the authorised authority connected it to a forensic workstation. The legal record produced under Article 160, which carries higher formality, requiring the investigating judge's presence and clerk's signature, creates a false sense of procedural completeness. The procedure is legally perfect at the physical objective level, while the evidential risk exists entirely at the intangible digital data level. Neither article contains any provision for forensic imaging<sup>10</sup>, hash verification<sup>11</sup>, or write-blocking<sup>12</sup>, the operations that constitute digital acquisition under international standards<sup>13</sup>. This limitation carries a direct nullity consequence. Article 109 of the CCP lists the provisions whose violation renders any resulting evidence null and void, and Articles 91 and 92 are explicitly enumerated in that list<sup>14</sup>. Because digital evidence acquisition necessarily deviates from the physical sealing procedure, current forensic practice requires that the Forensic Officer ('FO'<sup>15</sup>) must connect a phone to extraction hardware<sup>16</sup> and software<sup>17</sup>, copy data to a separate storage medium, and produce a hash-verified report, none of which is a 'sealing' in any legally recognised sense; consequently, a defence lawyer can characterise current practice as a violation of Article 92 and invoke Article 109 to have digital evidence declared null in theory. The gap, therefore, does not merely make evidence unreliable; it exposes all digitally acquired evidence to a structural nullity challenge that cannot be rebutted under current law. Three further provisions deepen the problem. Article 172, the CCP's principal provision substantively regulating the interception of digital communications, authorises the investigating judge to order the interception of telephone conversations, faxes, and emails, but covers only communications in transit, not data stored on seized devices. Meanwhile, Article 95 of the CCP allows judicial police officers, where an examination calls for

8 United Nations Office on Drugs and Crime, 'More than 0s and 1s: Cambodia Battles Cybercrime,' UNODC, 28 January 2025, [https://www.unodc.org/unodc/en/frontpage/2025/January/more-than-0s-and-1s\\_-cambodia-battles-cybercrime.html](https://www.unodc.org/unodc/en/frontpage/2025/January/more-than-0s-and-1s_-cambodia-battles-cybercrime.html); Business & Human Rights Resource Centre, 'Cambodia: UNODC's map alleges that Cambodia is a global hub for scamming operations with alleged companies linked to high ranking officials,' Business & Human Rights Resource Centre, 18 June 2025, <https://www.business-humanrights.org/en/latest-news/cambodia-unodcs-map-alleges-that-cambodia-is-a-global-hub-for-scamming-operations-with-alleged-companies-linked-to-high-ranking-officials/>.

9 Kingdom of Cambodia, Code of Criminal Procedure (2007), arts. 91, 92, 159, 160, 321.

10 Forensic imaging is the 'process of creating a bitwise copy of digital storage media,' also known as a physical copy, which captures all data including deleted files and unallocated space. See International Organization for Standardization, ISO/IEC 27037:2012 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (Geneva: ISO, 2012), §3.13.

11 Hash verification is the use of a verification function to confirm that two sets of data are identical, typically by computing and comparing hash values, where any alteration to the data produces a different hash value. See International Organization for Standardization, ISO/IEC 27037:2012, op. cit., §§3.11, 3.25.

12 Write-blocking is the use of technical methods, devices, or software that permit reading data from storage media while preventing any writing, modification, or addition to the source media, thereby preserving the original evidence in its unaltered state. See Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, Version 5 (2012), Principle 1.

13 International Organization for Standardization, ISO/IEC 27037:2012 op. cit., §5.4.4.

14 Kingdom of Cambodia, Code of Criminal Procedure, op. cit., art. 109. Article 109 provides that violations of Articles 91 and 92 render the resulting evidence null and void.

15 Forensic Officer ('FO') may be understood as the person who handles digital evidence. Under ISO/IEC 27037, a FO can be classified as 'Digital Evidence First Responder (DEFRR)' or, where greater specialisation is required, a 'Digital Evidence Specialist (DES)'. See International Organization for Standardization, ISO/IEC 27037:2012 op. cit., §§3.7–3.8.

16 Forensic hardware refers to the physical equipment used to acquire data from a seized device, including write-blockers, mobile-device forensic kits (such as Cellebrite UFED or MSAB XRY), JTAG/chip-off rigs, and dedicated forensic workstations with validated imaging capacity. See International Organization for Standardization, ISO/IEC 27037:2012, op. cit., §§5.4.4–5.4.5.

17 Forensic software refers to validated computer programs used to acquire, preserve, and analyse digital evidence in a forensically sound manner, including imaging tools (e.g. EnCase, FTK Imager, dd), mobile-extraction suites (e.g. Cellebrite UFED, Oxygen Forensics), and hash-verification utilities. See International Organization for Standardization, ISO/IEC 27037:2012, op. cit., §5.4.5.

technical knowledge they do not themselves hold, to engage qualified experts for a scientific examination<sup>18</sup> of seized items, and in the digital context it is the sole legal basis for tasking a Forensic Officer with examining a seized smartphone or computer, yet it sets no qualification criteria, no methodology requirements, and no standard for how a digital forensic report must be produced<sup>19</sup>. The reliance sometimes placed on the judge's intine conviction under Article 321 to evaluate such expert testimony does not cure this deficiency: Article 95 expertise operates at the stage of weighing evidence already admitted, and cannot substitute for the chain-of-custody documentation that gives any expert opinion its evidentiary foundation. Moreover, a successful nullity challenge under Article 109 excludes the evidence at the admissibility stage entirely, before the judge's evaluative discretion is ever engaged. Beyond these provisions, there is no rule governing the transport of seized digital devices from the scene to the National Police Commissioner of Cambodia's ('NPCC') forensic department, a legally significant gap, because electrostatic discharge, magnetic fields<sup>20</sup>, and physical shock during transport can irreparably damage digital storage media<sup>21</sup>. These limitations are compounded by a terminological inconsistency across the CCP, the Law on Electronic Commerce (2019) ('LEC'), and international standards, whose definitions are not interoperable<sup>22</sup>. Article 40 of the Constitution protects the secrecy of correspondence by mail, telegram, fax, telex, and telephone, an enumeration that contains no specific reference to digital data, and remains operationally dormant in the digital context because no procedural rule gives it force at the moment of digital data acquisition. Article 321, subject only to the qualifying clause 'unless it is provided otherwise by law,' admits all evidence on the judge's intimate conviction without any authentication threshold, depriving courts of any technical benchmark for evaluating digitally acquired evidence while leaving the qualifying language itself an enabling clause for the Anukret this brief proposes<sup>23</sup>. The combined effect is a framework where investigators<sup>24</sup> are legally exposed, defendants cannot mount a meaningful procedural challenge, and judges lack the tools to evaluate what is presented before the court.

### III. Comparative Jurisdictions Addressing the Procedural Gaps in Digital Evidence Acquisition

The remediability of the systemic gap identified in Section 1 through legislative reform is demonstrated by reference to jurisdictions that have addressed structurally similar problems. Three comparative sources, namely Singapore's Criminal Procedure Code ('SCPC'), the French Code de procédure pénale ('FCPP'), and the case law of the Court of Justice of the European Union, demonstrate that such reform is both legally feasible and practically achievable. These jurisdictions are drawn on because each operates a civil-law-influenced criminal procedure comparable to Cambodia's, and each has confronted the precise problem at issue here: how to give legal form to the interval between the physical seizure of a device and the acquisition of the data inside it. Singapore and France supply two legislative answers to that divide, while the Court of Justice supplies the rights framework against which any answer must be measured. The comparison is therefore not offered for its own sake but to identify which features of each model are transferable to Cambodia's prosecutor-and-investigating-judge structure and which are not. Section 39 of the SCPC grants the police the statutory power to access, inspect, and copy data from a seized computer, compel assistance from system users, and prevent third-party access. In addition, Section 116A of the Evidence Act creates rebuttable presumptions of authenticity for electronic records properly collected, linking collection quality directly to admissibility outcomes and incentivising procedural compliance<sup>25</sup>. Subsequently, Singapore courts have interpreted this framework in *Telemedia Pacific Group Ltd v Credit Agricole*, confirming the facilitative nature

18 The Code of Criminal Procedure does not define 'scientific examination' or fix the threshold an examination must meet to qualify as scientific, nor does it prescribe the qualifications, methodology, or reporting standard of the expert engaged under Article 95; the term is left to practice. See Kingdom of Cambodia, Code of Criminal Procedure, op. cit., art. 95.

19 Kingdom of Cambodia, Code of Criminal Procedure, op. cit., arts. 95, 172.

20 Electrostatic discharge is the sudden, uncontrolled flow of electric charge between two objects at different electrical potentials, which can corrupt or erase data held on memory chips and other storage components. A magnetic field, such as that produced by speakers, magnets, or scanning equipment, can disturb the magnetised regions by which hard-disk media encode data and so alter or destroy their contents. See International Organization for Standardization, ISO/IEC 27037:2012, op. cit.; INTERPOL, Guidelines for Digital Forensics First Responders, op. cit.

21 International Organization for Standardization, ISO/IEC 27037:2012, op. cit., §6.9.4.

22 The CCP uses 'exhibit' as a physical concept; the LEC uses 'electronic evidence' in commercial terms; ISO/IEC 27037 uses 'digital evidence' as a technical category. None of these definitions are interoperable. See Kingdom of Cambodia, LEC, art. 43 and Annex Definition 17.

23 Kingdom of Cambodia, Code of Criminal Procedure, op. cit., art. 321; cf. République française, Code de procédure pénale (2025), art. 427 (the parallel French formulation of the intine conviction doctrine).

24 Investigators in this context refer to the judicial police officer and the investigating judge. See Kingdom of Cambodia, Code of Criminal Procedure, op. cit., arts. 91, 92, 159, 160.

25 Republic of Singapore, Criminal Procedure Code 2010, §39; Evidence Act 1893 (as amended), §116A.

of Section 116A, and in *GIL v Public Prosecutor*, refining its scope for personal devices such as smartwatches<sup>26</sup>. The Singapore model demonstrates that specific statutory authorisation combined with an evidentiary presumption linked to proper collection can operate coherently within a civil-law-influenced procedural structure. By contrast, Article 57-1 of the FCPP treats the seizure of a digital device and the access to its data as two legally distinct acts, each requiring separate authorisation grounded in proportionality<sup>27</sup>. The device seizure is a property act; the data access is a privacy act.

This architecture recognises that these two acts implicate different fundamental rights and cannot be governed by a single rule. The French model responds directly to the gap between Cambodia's physical seizure under Articles 92 and 160 and the acquisition of digital data that follows. In *C.G. v Bezirkshauptmannschaft Landeck*, Austrian police seized a phone and attempted to access its data without authorisation, documentation, or notification, a factual pattern structurally identical to current Cambodian practice<sup>28</sup>.

The Grand Chamber of the Court of Justice of the European Union held that this constituted a serious interference with fundamental rights requiring prior authorisation, proportionality, and clear legal rules<sup>29</sup>. In *Comdribus*, the Court held that the collection of sensitive personal data must be strictly necessary, case-specific, and supported by written reasons<sup>30</sup>. Although Court of Justice jurisprudence is persuasive rather than binding on Cambodian courts, it offers a methodologically rigorous articulation of the proportionality and prior-authorisation safeguards that the procedural reform proposed here seeks to operationalise. Singapore's police-authorised model cannot be transplanted directly. Under Articles 91 and 159 of the CCP, the power to authorise searches and seizures and to handle exhibits rests exclusively with the Royal Prosecutor and the investigating judge. That dual-authorisation framework derives from the French judge d'instruction tradition, codified in FCPP Articles 92 and 94, which vest search and seizure powers in the investigating judge subject to prosecutorial notification. Singapore, by contrast, delegates those powers directly to police officers under Section 39 of the SCPC, with no equivalent judicial oversight. Its mechanism is therefore non-transferable without fundamental modification to Cambodia's authorisation structure. The French framework, in particular FCPP Article 57-1's separation of physical seizure from access to data on a system found at the scene of a search, presupposes an institutional infrastructure that exceeds Cambodia's immediate capacity, given the current absence of certified forensic specialists, accredited digital forensic laboratories, and standardised acquisition protocols capable of supporting the procedural rigour that model presupposes.

What is transplantable across all three jurisdictions is the underlying principle: the law must specify what investigators may do with data on a seized device, under what conditions, and with what documentation.

## IV. Five Principles to Govern Digital Evidence Acquisition in Cambodia

Closing the acquisition gap requires identifying the minimum legal standards any reform must embody. Five principles emerge from the convergence of ISO, the ACPO Good Practice Guide ('ACPO'), SCPC, FCPP, and recent jurisprudence. The first principle is legal authorisation for data access. Accessing data inside a seized device is a legally distinct act from seizing the device itself and requires specific authorisation identifying the categories of data sought. This principle directly addresses the gap in Articles 91 and 159 and gives operational force to the constitutional privacy guarantee of Article 40. The second principle is non-alteration. No action taken during acquisition should alter data on the original device, and where alteration is unavoidable, it must be documented with justification. This principle responds directly to the write-blocking gap exposed by Articles 92 and 160 and draws on Principle 1 of the ACPO<sup>31</sup>. The third principle is integrity verification. Cryptographic<sup>32</sup> hash values must be calculated and recorded for all extracted data, with the hash of the forensic copy verified against the hash of the original source. In procedural terms, the hash should be generated with a recognised algorithm such as SHA-256, computed on the source media before imaging and again on the forensic copy immediately after acquisition, with both values entered in the forensic report and the chain-of-custody record and re-verified before the evidence is tendered in court. A match confirms that the copy is identical to the source; any discrepancy must be recorded and accounted for rather than concealed. Hash verification is the functional digital equivalent of the physical seal required by Articles 92 and 160; it certifies the integrity of data in the way a wax seal certifies the integrity of a physical object. The fourth

26 *Telemedia Pacific Group Ltd v Credit Agricole (Suisse) SA* [2014] SGHC 235 (High Court of Singapore, 18 November 2014); *GIL v Public Prosecutor* [2024] SGHC 287 (General Division of the High Court of Singapore, 6 November 2024).

27 *République française*, Code de procédure pénale, op. cit., art. 57-1.

28 *C.G. v Bezirkshauptmannschaft Landeck*, Case C-548/21, ECLI:EU:C:2024:830 (CJEU Grand Chamber, 4 October 2024).

29 *C.G. v Bezirkshauptmannschaft Landeck*, op. cit., paras.107-120.

30 *Comdribus*, Case C-371/24, ECLI:EU:C:2026:219 (CJEU Fifth Chamber, 19 March 2026), paras.28-43.

31 Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, op. cit., Principle 1; INTERPOL, Guidelines for Digital Forensics First Responders, op. cit., p.34.

32 A cryptographic hash value is a fixed-length 'string of bits which is the output of a hash-function' (for instance MD5, SHA-1 or SHA-256), serving as a unique digital fingerprint of the source data; any alteration to the data, however small, produces a different hash value. See International Organization for Standardization, ISO/IEC 27037:2012 op. cit., §3.11.



principle is documentation and chain of custody. Every action taken on a seized device from the moment of seizure, through transport to the forensic headquarters<sup>33</sup>, to the completion of the forensic report must be recorded contemporaneously, identifying person, tool, time, and location. This principle addresses both the acquisition gap and the transport gap identified in Section 1 and aligns with ISO/IEC 27037 Section 6.1<sup>34</sup>. The fifth principle is proportionality of scope. Specifically, data extraction must be limited to data relevant to the specific offence under investigation, with each category of data documented as relevant. This principle operationalises the strict necessity standard articulated by the Court of Justice in *Comdribus* and gives concrete force to Article 40's privacy protection. These five principles are technology-neutral, drawn from converging international sources, and capable of phased adoption without new institutions. These principles respond directly to each gap identified in Section 1: Principles 1 and 5 address the authorisation and proportionality gaps; Principles 2 and 3 address the sealing and integrity gaps; Principle 4 addresses the documentation and transportation gaps. These principles do not resolve compelled decryption or cloud access, which require separate legislation, and they presuppose a minimum forensic capacity at the GCNP, which the KOICA investment is now building.

## V. An Anukret as the Realistic and Immediate Reform Pathway

The five principles identified in Section 3 require a legal instrument that is binding, timely, and institutionally achievable. Amendment of the Code of Criminal Procedure is politically slow and unnecessary, since the principles operationalise existing CCP provisions rather than replacing them. A new standalone law would create overlap and inconsistency with the CCP and the Law on Electronic Commerce. A Prakas has insufficient legal force to bind judicial police and investigating judges uniformly<sup>35</sup>. A Sub-Decree (Anukret), issued by the Council of Ministers under existing Royal Government authority, is binding on all officials, updateable as technology evolves, and appropriate subject matter for subordinate legislation<sup>36</sup>. The reform should proceed in two parts. The first part, addressed to the Royal Prosecutor and judicial police under existing prosecutorial directive authority, consists of immediate measures that can be implemented now without waiting for the Sub-Decree: mandatory documentation of every action taken on seized digital devices from the moment of seizure through transport to the forensic headquarters; mandatory write-blocking where available at the forensic headquarters; mandatory hash calculation and recording for all extracted data; and mandatory chain-of-custody records identifying handler, tool, time, and location. These measures directly reduce the nullity risk under Article 109 by bringing current practice closer to a defensible procedural standard. The second part, addressed to the Council of Ministers, consists of a Sub-Decree on Digital Evidence Collection operationalising Articles 91, 92, 159, and 160 of the CCP. The Sub-Decree should formally incorporate the five principles as legally binding standards; define digital evidence, forensic imaging, hash value, write-blocking, chain of custody, and digital forensic specialist; establish FO competency requirements aligned with ISO/IEC 27037; specify transportation and packaging standards for seized digital devices; and introduce a rebuttable presumption of authenticity for properly collected evidence, adapted from Singapore's Section 116A. The Sub-Decree should also resolve the terminological inconsistency across Cambodia's legal instruments by establishing 'digital evidence' as the operative legal term for all binary-format data requiring forensic handling. The proposal must be localised in the Cambodian reality. The Sub-Decree does not prohibit current informal investigative practice; it formalises and standardises it so that the resulting evidence becomes legally defensible under Article 109. Where a locked device requires technical bypass and no password is available, the Sub-Decree permits such bypass under prosecutorial authorisation, with contemporaneous documentation and hash verification. This accommodates Cambodian investigative culture and the practical realities of cybercrime enforcement while imposing the minimum legal structure necessary to eliminate the nullity risk, protect the rights of the accused, and make the output of the KOICA laboratory legally admissible in court.

## VI. Conclusion

The CCP was written for physical evidence. Articles 92 and 160 can seal a phone or computer but not its data. Article 109 threatens to void any evidence whose collection deviates from that physical seal. Article 321 admits everything, yet at the same time authenticates nothing. Together, these provisions create not merely a technical inconvenience but a procedural risk that, if left untouched, will expand its danger as digital evidence becomes a more central piece of the puzzle in Cambodian criminal proceedings. A Sub-Decree on Collection, Acquisition, and Presentation of Digital Evidence in Criminal Proceedings, grounded in five principles of authorisation, non-alteration, integrity verification, documentation, and proportionality, closes the

<sup>33</sup> Forensic Headquarters here refers to the GCNP.

<sup>34</sup> International Organization for Standardization, ISO/IEC 27037:2012, op. cit., §6.1.

<sup>35</sup> The present brief revisits and departs from the Prakas-based reform pathway considered in the author's previous work. See Odom Somnang, *From Bytes to Burden of Proof: Establishing Cambodia's Digital Evidence Framework*, KASFLY Law Brief 3.0, 2025.

<sup>36</sup> Kingdom of Cambodia, Constitution of the Kingdom of Cambodia (1993, as amended), arts. 118–119.

gap and risk without amending the CCP and without demanding institutional capacities that Cambodia does not yet possess. The immediate measure available under existing prosecutorial authority can begin reducing the nullity risk starting from now. The KOICA laboratory will soon produce technical and sophisticated forensic reports of the seized evidence. Without the legal framework proposed in this brief, those reports will remain vulnerable to challenge under Article 109 in every case where digital evidence bears the burden of proof. The infrastructure is arriving. The law should therefore arrive at the same destination. This brief has limited its analysis to the acquisition of data from seized smartphones and computers. Two analytically distinct procedural gaps fall outside the present scope and warrant separate scholarly treatment, particularly as Cambodia's institutional capacity matures: the acquisition of cloud-stored data subject to foreign jurisdictional and mutual legal assistance constraints, and compelled decryption in light of the privilege against self-incrimination. The principles articulated here may also serve as a foundation for subsequent inquiry into the admissibility consequences of trans-border digital evidence and into the procedural treatment of artificial-intelligence-generated evidence under Article 321.

## Bibliography

### Legislation

1. Kingdom of Cambodia. Code of Criminal Procedure. 2007.
2. Kingdom of Cambodia. Constitution of the Kingdom of Cambodia. 1993.
3. Kingdom of Cambodia. Law on Electronic Commerce. 2019.
4. Kingdom of Cambodia. Law on Combating Online Scams. 2026.
5. République française. Code de procédure pénale. 2025.
6. Republic of Singapore. Criminal Procedure Code. 2010.
7. Republic of Singapore. Evidence Act. 1893 (as amended).

### Case Law

1. C.G. v Bezirkshauptmannschaft Landeck, Case C-548/21, ECLI:EU:C:2024:830 (CJEU Grand Chamber, 4 October 2024).
2. Comdribus, Case C-371/24, ECLI:EU:C:2026:219 (CJEU Fifth Chamber, 19 March 2026).
3. GIL v Public Prosecutor [2024] SGHC 287 (General Division of the High Court of Singapore, 6 November 2024).
4. Telemedia Pacific Group Ltd v Credit Agricole (Suisse) SA [2014] SGHC 235 (High Court of Singapore, 18 November 2014).

### International Standards and Guidelines

1. Association of Chief Police Officers. ACPO Good Practice Guide for Digital Evidence, Version 5. 2012. International Organization for Standardization. ISO/IEC 27037:2012 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO, 2012.
2. INTERPOL. Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence. Lyon: INTERPOL General Secretariat, 2021. [https://www.interpol.int/content/download/16243/file/Guidelines\\_to\\_Digital\\_Forensics\\_First\\_Responders\\_V7.pdf](https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf).

### Books

1. Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Waltham, MA: Academic Press, 2011.
2. Holt, Thomas J., Adam M. Bossler, Kathryn C. Seigfried-Spellar. Cybercrime and Digital Forensics: An Introduction. 3rd ed. London: Routledge, 2022.

### Reports

1. United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. New York: United Nations, 2013.
2. United Nations Office on Drugs and Crime. 'More than 0s and 1s: Cambodia Battles Cybercrime.' UNODC, 28 January 2025. [https://www.unodc.org/unodc/en/frontpage/2025/January/more-than-0s-and-1s\\_-cambodia-battles-cybercrime.html](https://www.unodc.org/unodc/en/frontpage/2025/January/more-than-0s-and-1s_-cambodia-battles-cybercrime.html).
3. United Nations Office on Drugs and Crime. Electronic Evidence Fiche: Cambodia. SHERLOC Knowledge Management Portal. [https://www.unodc.org/cld/uploads/pdf/EI%20Evidence%20Hub/Electronic\\_Evidence\\_Fiche\\_as\\_of\\_18\\_January\\_CAMBODIA.pdf](https://www.unodc.org/cld/uploads/pdf/EI%20Evidence%20Hub/Electronic_Evidence_Fiche_as_of_18_January_CAMBODIA.pdf).
5. Business & Human Rights Resource Centre. 'Cambodia: UNODC's Map Alleges That Cambodia Is a Global Hub for Scamming Operations with Alleged Companies Linked to High-Ranking Officials.' June 18, 2025. <https://www.business-humanrights.org/en/latest-news/cambodia-unodcs-map-alleges-that-cambodia-is-a-global-hub-for-scamming-operations-with-alleged-companies-linked-to-high-ranking-officials/>.

## News Articles

1. Khmer Times. 'Forensic Investigation Capacity Gets \$13.5 Million Boost.' Khmer Times, 1 April 2026. <https://www.khmertimeskh.com/501872247/forensic-investigation-capacity-gets-13-5-million-boost/>.
2. The Phnom Penh Post. 'Tightening the Net: Anti-Tech Scam Law Rolled Out Nationwide.' The Phnom Penh Post, 7 April 2026. <https://phnompenhpost.com/national/tightening-the-net-anti-tech-scam-law-rolled-out-nationwide/>.



## **Confiscation of Digital Assets under Cambodian Criminal Proceedings: Procedural Gaps and Enforcement Challenges**

*YIN Hongleang*



## Abstract

The growing use of digital assets in criminal activities has posed new challenges for criminal confiscation proceedings. Under Cambodian laws and regulations, have the mechanism in place to freeze, seize, and confiscate criminal property. Nevertheless, these remain uncertain due to their unique characteristics, including decentralization and rapid transferability across borders in seconds.

This brief aims to explore procedural gaps and enforcement challenges in the confiscation of digital assets in Cambodia. The brief also further addresses the issues arising throughout the confiscation process, starting from orders, taking control over those digital assets, and cross-border cooperation through mutual legal assistance.

Procedural approaches from best practices in Singapore, Poland, and the European Union have the potential to complement the current framework of Cambodia. This brief suggests that Cambodia should develop clearer procedural rules for preserving, securing, and enforcing confiscation over digital assets, at the same time as enhancing international cooperation. Strengthening these procedural mechanisms would have had the important functions of improving legal certainty, increasing the practical effectiveness of confiscation proceedings, and better equipping Cambodia's criminal justice system to respond to crimes involving digital assets.

## I. Introduction

The evolving nature of transnational technology-enabled crime has expanded in both scale and complexity, resulting in a significant increase in cross-border victimization<sup>1</sup>, and digital assets have increasingly been used to facilitate a growing range of crimes, including various fraud schemes and ransomware<sup>2</sup>. Cambodia is one of many countries in the region where criminals operate online scams; this has contributed to the growing concerns about public safety and the need for stronger legal measures to protect citizens<sup>3</sup>. To address these issues, Cambodia has recently adopted the Law on Combating Technology-Enabled Scam (“**LCTES**”), which aims to establish criminal provisions to enhance the effectiveness of protecting security, public social order, and to strengthen cooperation in combating these crimes<sup>4</sup>. Although the procedures governing these matters are provided under the Cambodia Code of Criminal Procedure (“**CCP**”) and Law on Mutual Legal Assistance in Criminal Matters (“**LMLACM**”) to recognize freezing, seizure, and confiscation of assets connected to criminal activities<sup>5</sup>, the procedural question of how to confiscate digital assets remains insufficiently addressed. This issue becomes increasingly important as digital assets are increasingly used to facilitate crime<sup>6</sup>, while Cambodian law does not have a comprehensive legal procedure for these types of assets. Accordingly, this paper will discuss the critical legal challenges and procedural barriers by elaborating on (1) the statutory incongruity, (2) practical challenges in preserving and executing confiscation, and (3) Mutual Legal Assistance (“**MLA**”) in the freezing and confiscation.

## II. Statutory Incongruity: Conceptualizing Digital Assets Within Cambodia's Confiscation Framework

Under the Cambodia Criminal Code (“**CCC**”), confiscation may be ordered in relation to any instruments, materials or items which were used or intended to be used to commit the offence, the items or funds which were the subject of the offence, the proceeds or property arising out of the offence, the utensils, materials, and furnishings in the premises in which the offence was committed<sup>7</sup>.

1 Global Consortium Group, “What Is Cybercrime in Today's World and What Does the Future Hold for Law Enforcement?,” accessed June 11, 2026, <https://www.globalconsortiumgroup.com/what-is-cybercrime-in-todays-world-and-what-does-the-future-hold-for-law-enforcement>

2 United States Secret Service, “Digital Assets,” Secretservice.gov, 2024, <https://www.secretservice.gov/investigations/digitalassets>.

3 Xinhua, “Cambodia's parliament adopts law on combating online scams, with life imprisonment for scam bosses 2026” March 30, 2026, accessed April 20, 2026, <https://english.news.cn/20260330/3d64f1137e734c15861ddc3c25c5a66a/c.html>.

4 Fresh News, “Cambodia Promulgates Law on Combating Technology-Enabled Scam,” April 7, 2026 <https://m.en.fresh-newsasia.com/index.php/en/localnews/69527-2026-04-07-07-38-38.html>; Raksmei Hong, “Cambodian Embassy Defends Kingdom's Anti-Scam Record, Cites over 13,000 Deportations,” Phnom Penh Post, May 15, 2026, <https://phnompenhpost.com/national/cambodian-embassy-defends-kingdoms-anti-scam-record-cites-over-13000-deportations/>.

5 Sub-Section 7, Article 30-34. Law on Mutual Legal Assistance in Criminal Matters (“**LMLACM**”), 27 June 2020.

6 Tran Duy Canh and Ling Yi Quek, “Overview on Digital Assets Regulations in SEA,” Rodyk.com, 2022, <https://dentons.rodyk.com/en/insights/alerts/2022/july/6/overview-on-digital-assets-regulations-in-sea>.

7 Art. 178, Cambodia Criminal Code, (2009).

To execute these substantive measures, the CCP empowers an authorized investigating judge to seize confiscated exhibits, seal them, prepare inventories, and record the confiscation processes<sup>8</sup>. This traditional framework was recently supplemented by the Law on Combating Technology-Enabled Scams (“**LCTES**”), which also provides a mechanism. Upon detecting properties or suspicious transactions related to the offenses or the proceeds of crime, a judicial police officer may request competent authorities to temporarily seize the property or suspend the transactions. Specifically, it requires the competent authorities to take immediate action to temporarily seize the property or suspend the transactions to safeguard the future enforcement of a claim or prevent imminent harm to disputed rights<sup>9</sup>. However, the common form of such orders may appear to have been designed primarily for tangible assets and assets under banking and financial systems, which may not be readily applicable to digital assets.

According to the Cambodia Financial Technology Development Policy 2023-2028, “Digital Asset” refers to a valuable digital unit created on distributed ledger technology or similar technology or associated with a smart contract or contract in the various forms between digital asset holders and counterparts, which can be traded or transferred, including Bitcoin, and are the financial instruments that are a type of securities<sup>10</sup>. In practice, it is commonly used to transfer value between individuals or businesses without involving a bank, to store wealth outside traditional banking systems, and to pay for cross-border transactions<sup>11</sup>.

Crucially, the foundation of this asset ownership depends on the public key operating similarly to a bank account number or email address, which can be freely shared with others who want to send cryptocurrency and appear on the public blockchain. Conversely, a private key is a string of alphanumeric characters that functions as the master password to a digital vault<sup>12</sup>. Those who possess a private key have complete control over the cryptocurrency associated with it. It operates without intermediaries; if the private key is lost or someone else obtains it, the consequences can be financially devastating and legally complicated<sup>13</sup>. This uncertainty becomes particularly significant because digital assets may rapidly fluctuate in value, be transferred across jurisdictions within seconds, or become inaccessible where the relevant private keys cannot be obtained by the authorities<sup>14</sup>.

Unlike traditional assets, digital assets can be exchanged via blockchain networks without necessarily revealing the name of the person in control, in contrast to traditional assets that are connected to identifiable owners through bank accounts, registration systems, or physical possession<sup>15</sup>. This anonymity allows illicit proceeds to be dispersed through layers of transactions intended to conceal ownership and transactional history. With Cambodia’s existing law, it empowers prosecutors to seek court orders to freeze accounts, and financial authorities are allowed to freeze suspicious transactions via the Cambodia Financial Intelligence Unit (**CAFIU**)<sup>16</sup>. Furthermore, the National Bank of Cambodia also just issued the Prakas B7-024-735 on Transactions Related to Crypto Assets to manage the transaction boundaries and business activities<sup>17</sup>. However, it offers little procedural guidance on how to use cryptocurrency wallet data, blockchain transaction records, and evidence from intermediary institutions to prove ownership or control of a digital asset during confiscation proceedings. The absence of a procedure to access private keys and identify the ownership may reduce the effectiveness of confiscation measures, even when the authorities have the authorized power to confiscate that kind of asset from the accused person.

Under the jurisdiction of Singapore, asset recovery is considered an element of the national strategy for combating financial crime. The National Asset Recovery Strategy emphasizes the need for early identification and retention of assets, as well as coordination between financial intelligence, law enforcement, and regulators<sup>18</sup>.

Given this nature, digital assets may fall within the broad concept of property, which could be counted as

8 Art 92, Cambodia Code of Criminal Procedure (“CCP”), (2007).

9 Art 19, LCTES.

10 Cambodia Financial Technology Development Policy 2023-2028, Annex 2. Glossary, Page 38.

11 Chainalysis, “*Cryptoasset Realization Explained*,” Chainalysis Blog, accessed June 20, 2026, <https://www.chainalysis.com/blog/cryptoasset-realization-explained/>

12 FinTech Weekly, “*How a Crypto Wallet Gives Full Control over Digital Assets*,” FinTech Magazine Article (FinTech Weekly, August 27, 2025), <https://www.fintechweekly.com/magazine/articles/crypto-wallet-control-over-digital-assets>.

13 Glendale Law Office, “*Understanding Cryptocurrency Private Keys: Legal Protection for Digital Asset Owners*,” The bulldog. law, December 17, 2025, <http://thebulldog.law/understanding-cryptocurrency-private-keys-legal-protection-for-digital-asset-owners>.

14 The Law Society, “*Introduction to digital assets*,” (The Law Society, February 4, 2026), <https://www.lawsociety.org.uk/topics/ai-and-lawtech/introduction-to-digital-assets#sub-menu-dy7>.

15 *Ibid*.

16 Art 19, LCTES.

17 Chapter I, Art 1-3, Prakas on Transactions Related to Crypto Assets, 26 December, 2024.

18 Ministry of Home Affairs, Ministry of Finance Singapore, and Monetary Authority of Singapore, “*National Asset Recovery Strategy 2024*,” n.d., [https://acd.mlaw.gov.sg/files/National\\_Asset\\_Recovery\\_Strategy\\_2024.pdf..p.4](https://acd.mlaw.gov.sg/files/National_Asset_Recovery_Strategy_2024.pdf..p.4).

criminal proceeds under Cambodian law. However, while Cambodian law provides a general legal basis for confiscation, the absence of clear procedures for handling digital assets creates uncertainty necessary to take action on confiscation proceedings, even though Cambodia has the essential investigative and preservation tools.

To bridge this operational gap, it is suggested that the judicial authority, the Cambodia Financial Intelligence Unit (“**CAFIU**”), and the Ministry of Posts and Telecommunications (“**MPTC**”) collaborate in a joint effort to issue procedural guidelines on obtaining control and executing confiscation over digital assets. The proposed instruments should specifically address guidelines for dealing with the constraints of public and private keys and implement technology with the capability to record and track transactions of digital assets on blockchain. These guidelines would enhance the effectiveness of the enforcement mechanism that Cambodia already possesses. Additionally, the practical efficacy of the justice system would be enhanced by empowering the authority in charge with specialized training and knowledge in tackling this type of technology.

### III. Practical Challenges in Preserving and Executing Confiscation of Digital Assets

Under the Cambodia Code of Criminal Procedure (CCP), when the primary investigation involves a felony or misdemeanor, judicial police officers may conduct a search and seize relevant exhibits<sup>19</sup>. Digital wallets and cryptocurrency, which are forms of digital assets, often involve layered transactions. This complexity creates a practical challenge for the authority to take control of its transactions. Based on the report by the Cambodian Deputy Prime Minister and Minister of the Interior, H.E. Sar Sokha, in 2025, Cambodian citizens lost more than \$45 million to domestic online scams, and less than \$20 million was recovered, leaving the majority permanently lost<sup>20</sup>. The effort in the recovery of stolen funds is primarily hindered because syndicates are able to move funds across international borders in seconds<sup>21</sup>. Furthermore, given its global phenomenon, cross-border in its application, easily accessible, transferable, exchangeable, and tradable from nearly anywhere in the world<sup>22</sup>. These characteristics of digital transactions create significant challenges in obtaining control and executing during confiscation proceedings.

A useful model can be observed under the jurisdiction of Poland in cryptocurrency seizure and asset forfeiture, where Polish authorities have intensified their focus on cryptocurrency-related crimes<sup>23</sup>. The legal framework for cryptocurrency seizure in Poland is practically similar to that in Cambodia, which is primarily governed by the Criminal Procedure Code, the Anti-Money Laundering and Counter-Terrorist Financing Act, and the Polish Financial Supervision Authority<sup>24</sup>. In their practice, although cryptocurrency is not explicitly mentioned in provisions of the procedure law, Polish courts have consistently included digital assets as property subject to seizure. Besides that, they have also issued guidelines clarifying that cryptocurrencies may be subject to asset forfeiture proceedings when connected to criminal activities. These regulatory frameworks collectively establish a comprehensive legal basis for authorities to seize and confiscate digital assets potentially. Furthermore, in their enforcement, they have applied the technical implementation of seizing cryptocurrency generally following one of three approaches, such as forced transfer of assets to government-controlled wallets, Court-ordered disclosure of private keys by suspects, and freezing of assets held on regulated exchanges through direct cooperation with these entities.

Extending to that, based on the Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets (“**GAFILAT**”), the only way to safeguard the State authorities’ ability to seize digital assets is to transfer them to a wallet controlled by State authorities as soon as possible<sup>25</sup>. It prevents a third party or accused person from removing the funds before they can pass into the hands of the State<sup>26</sup>. Thus, the management of seized digital assets is a crucial measure to ensure the success of confiscation pending final judgement.

19 Art 113, CCP.

20 Khmer Times, 18 February 2026, “Online scams cost Cambodians \$45 million in 2025 as official warns of suicide risk” accessed via <https://www.khmertimeskh.com/501847531/online-scams-cost-cambodians-45-million-in-2025-as-official-warns-of-suicide-risk/#:~:text=The%20Minister%20said%20gravely%20that,within%20a%20staggering%20global%20con-text>.

21 Agence Kampuchea Presse (AKP), Phnom Penh, 17 February 2026, “Cambodians Lose US\$45M in 2025 as Interior Minister Warns of Deadlier Online Scams”, accessed via : <https://akp.gov.kh/post/detail/362458>.

22 KOPEC & ZABOROWSKI LAW FIRM, “Cryptocurrency Seizure and Asset Forfeiture in Poland: Legal Challenges and Defence Strategies | Criminal Law Poland,” Criminal Law Poland, November 17, 2025, <https://criminallawpoland.com/advice/cryptocurrency-seizure-and-asset-forfeiture-in-poland-legal-challenges-and-defence-strategies/>.

23 Robby Houben, Alexander Snyers, Crypto-assets: Key developments, regulatory concerns and responses, (Luxembourg: European Parliament, 2020), p.10.

24 *Ibid*.

25 GAFILAT, “Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets December 2021,” n.d., <https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets.pdf>. para 76, p 131 -132.

26 *Ibid*.

A lesson learned that Cambodia can take from these jurisdictions is to consider establishing government-controlled wallets and an authority governing a digital wallet to be able to securely preserve digital assets subject to preservation or confiscation orders. Moreover, it is suggested to observe the technical implementation by the Polish authorities of their ability to seize cryptocurrency. Lastly, it is suggested that the CAFIU and the judiciary strengthen their cooperation on financial regulation enforcement. With this cooperation, it could reduce the number of proceedings by establishing a mechanism that is able to expedite the process to seize control once the illicit transaction is discovered.

#### IV. MLA in the Freezing and Confiscation of Digital Assets

Under the Cambodian existing legal framework, even with or without any agreement, the procedure for Legal assistance in criminal matters to be provided or sought is set in the LMLACM<sup>27</sup>, which the Ministry of Justice (“MOJ”) serves as the central authority<sup>28</sup>. The LMLACM provides the proceedings related to freezing, seizure, and confiscation of property that are instruments of an offense used for the commission of an offense, or the proceeds of crime<sup>29</sup>. However, in the case of decentralized assets, digital assets can move across jurisdictions within seconds via transaction<sup>30</sup>, while LMLACM needs to process through a layer of procedures that often require a period of time to process. Therefore, this timing mismatch creates a risk that assets disappear before the execution of the order.

A useful model addressing this challenge can be observed under the jurisdiction of the Singaporean Court at the Singapore High Court decision in CLM v. CLN and others [2022] SGHC 46<sup>31</sup>. In this case, the plaintiff, an American citizen<sup>32</sup>, became the victim of cryptocurrency theft through an online scam and filed the lawsuit in a Singaporean Court because part of the stolen cryptocurrency and the intermediary accounts used in the fraudulent transactions were connected to Singapore-based cryptocurrency exchanges and financial infrastructure<sup>33</sup>. The Singapore High Court granted proprietary injunctions, worldwide freezing orders, also known as Mareva Injunctions<sup>34</sup>, and disclosure orders against cryptocurrency exchanges to facilitate tracing and recovery of the stolen digital assets<sup>35</sup>. Furthermore, the Court recognized cryptocurrency as property capable of proprietary protection and permitted proceedings against “persons unknown”<sup>36</sup>. This legal mechanism enabled the victim to pursue recovery even where the identities of the perpetrators remained uncertain, yet all transactions to and from can be viewed on the public blockchain<sup>37</sup>. Additionally, Singapore operates a centralized system in which the Attorney-General’s Chambers serves as the designated authority for handling MLA requests and ensuring clarity in both initiation and coordination<sup>38</sup>.

Within the European Union (“EU”) jurisdiction, regional law is equipped with a mechanism for cross-border asset enforcement. For instance, EU Regulation 2018/1805 ensures the mutual recognition of freezing and confiscation orders among Member States. This framework obligated member states to execute the foreign freezing orders within strict and mandatory deadlines, which could ensure that the assets in the cross-border proceeding are more effectively handled<sup>39</sup>. These processes are consistent with international standards reflected in instruments such as the United Nations Convention against Transnational Organized Crime (UNTOC), particularly Article 12, which requires States Parties to adopt to the maximum extent possible within their domestic legal systems, measures necessary to facilitate effective confiscation<sup>40</sup>.

Consequently, Cambodia can learn from the practice implemented by Singaporean courts in terms of proprietary injunctions, worldwide freezing orders, a centralized system, as well as proceedings against “persons unknown”, which are the operational lessons in practical enforceability. Besides this, even though Cambodia is not part of a regional legal regime with the same level of supranational integration as the EU, Cambodia, through ASEAN, could still strengthen cross-border cooperation. To achieve this, it is recommended that

27 Art.2 of LMLACM

28 Art. 4 of LMLACM

29 Art. 19 of LMLACM

30 “INTERPOL Silver Notices: Speeding up the Tracing of Criminal Assets” Basel Institute On Governance, March 16, 2026, <https://baselgovernance.org/resources/news/interpol-silver-notices-speeding-up-the-tracing-of-criminal-assets-2944/>.

31 The High Court of the Republic of Singapore, CLM vs. CLN and Other (March 4, 2022), [https://www.elitigation.sg/gd/s/2022\\_sghc\\_46](https://www.elitigation.sg/gd/s/2022_sghc_46).

32 *Ibid*, Para 6

33 *Ibid*, Para 55

34 *Ibid*, Para 50-56

35 *Ibid*, Para 60

36 Peter Doraisamy and PD LEGAL Singapore, “CASE SUMMARY : CLM v. CLN and Others [2022] SGHC 46,” PDLegal LLC, March 21, 2022, <https://www.pdlegal.com.sg/case-summary-clm-v-cln-and-others-2022-sghc-46>.

37 CLM vs. CLN and other, The High Court of the the Republic of Singapore, 2021, Plaintiffs’ 1st Affidavit dated 27 May 2021 at para 17

38 Singapore. Mutual Assistance in Criminal Matters Act (Revised Edition 2000, Division. 3.

39 European Commission, “Confiscation and Freezing of Assets” <https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/confiscation-and-freezing-assets>

40 Art 12, United Nations Convention against Transnational Organized Crime (UNTOC), 2000, Art. 16, Law on Mutual Legal Assistance in Criminal Matters, 27 June 2020.

Cambodian authorities develop clearer statutes within a specialized digital asset MLA protocol and establish procedures for urgent freezing requests. These mechanisms would provide competent authorities with clear guidance to manage and be able to take action toward illicit assets effectively and efficiently, especially when involving cross-border barriers.

## **V. Conclusion**

The emergence of new forms of technology creates more complexity in the existing legal frameworks, with digital assets now serving as one of the main means of financial transactions. At the same time, it is also an instrument for criminals to use as a means for their operation. Consequently, the capacity to effectively manage and confiscate these digital assets during criminal proceedings plays a crucial role in modern law enforcement. By establishing clear procedural guidelines, judicial authorities may be able to reduce crime related to digital asset transactions and leave less room for illicit operations where criminals attempt to evade detection.

Accordingly, to the extent of the evolving nature of new financial technology, the Cambodian asset-recovery framework may need to be reinforced to be fully sufficient to manage the complex, rapid evolution of these emerging technologies. Thus, adopting specific procedural mechanisms inspired by the operational models of Singapore, Poland, and the European Union represents a highly valuable legislative pathway. In addition to that, it is suggested that judicial authorities, CAFIU, and the MPTC collaborate on developing quick procedural mechanisms for tracking blockchain transactions, managing private key constraints, and establishing secure government-controlled digital wallets to preserve seized assets. These procedures and the practices and strategies implemented within those foreign jurisdictions and developments in the existing framework offer practical blueprints that can empower Cambodian authorities with practical enforceability and mechanisms in dealing with the evolving nature of the crime. And importantly, this mechanism will introduce new practical enforceability, which the prior enforcement may have had less impact.



## Bibliography

### Legislation

1. Cambodia Code of Criminal Procedure
2. Cambodia Criminal Code
3. Cambodia Financial Technology Development Policy 2023-2028
4. European Commission Regulation 2018/1805 on "Confiscation and Freezing of Assets"
5. Law on Combating Technology-Enabled Scam
6. Law on Mutual Legal Assistance in Criminal Matters
7. Monetary Authority of Singapore, National Asset Recovery Strategy
8. National Bank of Cambodia Prakas on Transactions Related to Crypto Assets
9. Poland Anti-Money Laundering and Counter-Terrorist Financing Act
10. Poland Criminal Procedure Code
11. Singapore Mutual Assistance in Criminal Matters Act
12. United Nations Convention against Transnational Organized Crime

### Case Law

1. The High Court of the Republic of Singapore. CLM vs. CLN and Other (March 4, 2022)
2. Peter Doraisamy, and PD LEGAL Singapore. "CASE SUMMARY: CLM v. CLN and Others [2022] SGHC 46." PD-LEGAL LLC, March 21, 2022. <https://www.pdlegal.com.sg/case-summary-clm-v-cln-and-others-2022-sghc-46>.

### Books, Journals, Articles, Reports

1. GAFILAT. "Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets December 2021," n.d. <https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets.pdf>.
2. Khiaonarong, Tanai, and Shanyuan Zheng. "The Rise of Cyber Events and Digital Fraud in the Financial Sector." IMF Elibrary, March 27, 2026. <https://doi.org/10.5089/9798229043557.001.a001>.
3. Prof. Dr. Robby HOUBEN, and Alexander SNYERS. "Crypto-Assets Key Developments, Regulatory Concerns and Responses," April 2020. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL\\_STU\(2020\)648779\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf).

### News Article, Blog and Website

1. Agence Kampuchea Presse (AKP), Phnom Penh, "Cambodians Lose US\$45M in 2025 as Interior Minister Warns of Deadlier Online Scams", 17 February 2026, accessed via: <https://akp.gov.kh/post/detail/362458>.
2. BASEL INSTITUTE ON GOVERNANCE. "INTERPOL Silver Notices: Speeding up the Tracing of Criminal Assets." BASEL INSTITUTE on GOVERNANCE (blog), March 16, 2026. <https://baselgovernance.org/resources/news/interpol-silver-notices-speeding-up-the-tracing-of-criminal-assets-2944/>.
3. Canh, Tran Duy, and Ling Yi Quek. "Overview on Digital Assets Regulations in SEA." Rodyk.com, July 22, 2022. <https://dentons.rodyk.com/en/insights/alerts/2022/july/6/overview-on-digital-assets-regulations-in-sea>.
4. FRESH NEWS. "Cambodia's New Law on Combating Technology-Based Fraud Promulgated," April 7, 2026. <https://m.en.freshnewsasia.com/index.php/en/localnews/69527-2026-04-07-07-38-38.html>.
5. Hong, Raksmeay. "Cambodian Embassy Defends Kingdom's Anti-Scam Record, Cites over 13,000 Deportations." phnompenhpost.com, May 15, 2026. <https://phnompenhpost.com/national/cambodian-embassy-defends-kingdoms-anti-scam-record-cites-over-13000-deportations/>.
6. Khmer Times, "Online scams cost Cambodians \$45 million in 2025 as official warns of suicide risk" 18 February 2026 accesss via <https://www.khmertimeskh.com/501847531/online-scams-cost-cambodians-45-million-in-2025-as-official-warns-of-suicide-risk>.
7. Kiripost. "Cambodians Scammed out of \$45M in Domestic Scams in 2025." Kiripost, February 19, 2025. <https://kiripost.com/stories/cambodians-scammed-out-of-45m-in-domestic-scams-in-2025>.
8. KOPEC & ZABOROWSKI LAW FIRM "Cryptocurrency Seizure and Asset Forfeiture in Poland: Legal Challenges and Defence Strategies | Criminal Law Poland." Criminal Law Poland, November 17, 2025. <https://criminallawpoland.com/advice/cryptocurrency-seizure-and-asset-forfeiture-in-poland-legal-challenges-and-defence-strategies/>.

9. Office, Glendale Law. "Understanding Cryptocurrency Private Keys: Legal Protection for Digital Asset Owners." Thebulldog.law, December 17, 2025. <http://thebulldog.law/understanding-cryptocurrency-private-keys-legal-protection-for-digital-asset-owners>.
10. Secret Service, United States. "Digital Assets." Secretservice.gov, 2024. <https://www.secretservice.gov/investigations/digitalassets>.
11. The Law Society. "The Law Society." @thelawsociety. The Law Society, February 4, 2026. <https://www.lawsociety.org.uk/topics/ai-and-lawtech/introduction-to-digital-assets#sub-menu-dy7>.
12. Today's, in. "Global Consortium Group." Global Consortium Group, 2025. <https://www.globalconsortiumgroup.com/what-is-cybercrime-in-todays-world-and-what-does-the-future-hold-for-law-enforcement>.
13. Weekly, FinTech. "How a Crypto Wallet Gives Full Control over Digital Assets." FinTech Magazine Article. FinTech Weekly, August 27, 2025. <https://www.fintechweekly.com/magazine/articles/crypto-wallet-control-over-digital-assets>
14. XINHUANET. "Cambodia's Parliament Adopts Law on Combating Online Scams, with Life Imprisonment for Scam Bosses." News.cn, 2026. <https://english.news.cn/20260330/3d64f1137e734c15861ddc3c25c5a66a/c.html>.
15. Youdy Bun, Boseihak Lay, Bun & Associates. "Client Alert: Cambodia's Draft Law on Combating Technology-Base Fraud Approved," n.d. <https://www.bun-associates.com/insight/783/client-alert-cambodias-draft-law-on-combating-technology-base-fraud-approved>.



## **Cybersecurity Incident Reporting in Cambodia's Banking Sector:**

### **Addressing Regulatory Fragmentation and Institutional Coordination**

*BON Somrach*



## I. Introduction

In line with regional and global trends, digital transformation is widely recognized as a strategic driver for accelerating the growth of the digital economy<sup>1</sup>. In accordance with the Royal Government of Cambodia's Pentagonal Strategy Phase I, the state has actively prioritized digital adoption as a key national strategy to foster a competitive digital economy and society<sup>2</sup>. This vision is further reinforced through the Cambodia Digital Economy and Society Policy Framework 2021-2035<sup>3</sup> and the Digital Government Policy 2022-2035<sup>4</sup>. Both policy frameworks have emphasized digital trust, secure transaction infrastructure and robust cybersecurity as foundational pillars for sustainable state development. Within this policy framework, the National Bank of Cambodia (NBC) has deployed a blockchain-based Bakong payment system, positioning Cambodia at a progressive stage in retail and wholesale payment system modernization across the ASEAN region<sup>5</sup>.

Nevertheless, cyberattacks against the financial sector have increased markedly in both frequency and sophistication over the past two decades, with new and increasingly complex attack typologies emerging<sup>6</sup>. Cyber incidents such as distributed denial-of-service (DDoS) attacks, advanced ransomware, coordinated phishing campaigns, insider threats, and systemic data breaches no longer represent isolated operational concerns<sup>7</sup>.

Cybersecurity is frequently characterized as a "wicked problem"<sup>8</sup>; it presents evolving threats across jurisdictional boundaries, resisting simple technical or unilateral regulatory solutions. In response to this, in early 2026, NBC promulgated the Technology and Cybersecurity Risk Management Guideline (TCRMG), which complements the 2019 Technology Risk Management Guidelines to impose rigorous, risk-based security expectations on all Banks and Financial Institutions (BFIs<sup>9</sup>). Concurrently, the Ministry of Post and Telecommunications (MPTC) released the Draft Law on Cybersecurity (Draft Law), introducing a centralized national governance model targeting Critical Information Infrastructure (CII) across ten essential sectors, including the banking and financial sector<sup>10</sup>.

The frameworks aim to protect Cambodia's digital space and build trust in digital technology, which is crucial for the growth of the digital economy, as stated in general<sup>11</sup> in the final sector-specific sector<sup>12</sup>. However, both frameworks state the same obligation regarding the Cyber Incident Report requirement. This may lead to duplicate reporting obligations, inconsistent regulations, delays in incident response coordination, and inefficiency in cybersecurity oversight. This Law Brief examines the fragmented incident reporting and analyses the legal and operational challenges arising from the interaction between the MPTC's national cybersecurity framework and the NBC's sector-specific regulation. It further proposes a sector-focused, nationally coordinated reporting model that preserves sector-specific expertise while improving national cybersecurity coordination and incident response.

1 Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, Introduction, p.

1; National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026, Introduction, p. 2; Sinawong Sang, Kong Phallack, Ou Phannarith, and Chhem Siriwat, "Cybersecurity Legislation: Policy Instrument to Improve Cybersecurity Readiness and Resilience," in Cambodia in Cyberspace: Anthology, ed. Siriwat Chhem, Ou Phannarith, and Chea Vatana (Phnom Penh: Asian Vision Institute, 2022) p. 97.

2 Royal Government of Cambodia, Pentagonal Strategy Phase I: For Growth, Employment, Equity, Efficiency and Sustainability (Phnom Penh: Council of Ministers, August 2023), p. 13.

3 Supreme National Economic Council, Cambodia Digital Economy and Society Policy Framework 2021-2035 (Phnom Penh: RGC, 2021), p. 8. <https://www.mptc.gov.kh/wp-content/uploads/2021/06/Cambodia-Digital-Economy-and-Society-Policy-Framework-2021-2035.pdf>.

4 Ministry of Post and Telecommunications, Digital Government Policy 2022-2035 (Phnom Penh: MPTC, 2022), p. 5. <https://mptc.gov.kh/wp-content/uploads/2022/03/Digital-Government-Policy-2022-2035-EN.pdf>.

5 National Bank of Cambodia, Financial Stability Report 2025 (Phnom Penh: National Bank of Cambodia, 2025), p. 31. [https://www.nbc.gov.kh/download\\_files/publication/fsr\\_eng/FSR2025\\_En.pdf](https://www.nbc.gov.kh/download_files/publication/fsr_eng/FSR2025_En.pdf).

6 ASEAN, ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace (2025), [https://asean.org/wp-content/uploads/2025/02/ASEAN\\_checklist\\_print.pdf](https://asean.org/wp-content/uploads/2025/02/ASEAN_checklist_print.pdf) (accessed January 23, 2026).

7 OECD, "Cybersecurity and Geopolitical Risks in Financial Markets," OECD Business and Finance Policy Papers (Paris: OECD Publishing, 2026), p. 11., [https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/cybersecurity-and-geopolitical-risks-in-financial-markets\\_e7efd32a/1002b1fd-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/cybersecurity-and-geopolitical-risks-in-financial-markets_e7efd32a/1002b1fd-en.pdf).

8 Chris Jay Hoofnagle and Golden G. Richard III, Cybersecurity in Context: Technology, Policy, and Law (Hoboken, NJ: Wiley, 2025), pp. 29-30.

9 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026 (Phnom Penh: National Bank of Cambodia, 2026), Introduction, p. 2.

10 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," in Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond, ed. Phallack Kong and Thomas Honnet (Phnom Penh: Konrad-Adenauer-Stiftung Cambodia, 2023), pp. 104-115.

11 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," in Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond, ed. Phallack Kong and Thomas Honnet (Phnom Penh: Konrad-Adenauer-Stiftung Cambodia, 2023), pp. 106.

12 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026 (Phnom Penh: National Bank of Cambodia, 2026), Introduction, p. 2.

## II. Conceptual Framework of Cambodia's Incident Reporting

A “Cyber Incident” is a potential jeopardy to the confidentiality, integrity, and availability of an information system or system processes or an imminent threat of violation of security policies<sup>13</sup>. In the banking sector, cyber incident offences are seen in the form of malware, fraud, intrusion, web threats, ransomware, social engineering, data-related threats, phishing, and distributed denial-of-services attacks<sup>14</sup>. In Cambodia, a cyber incident is a possible breach of security policy or a security situation that has a significant risk of damaging business operations<sup>15</sup>.

According to the NIST Cybersecurity Framework (**NIST 2.0**), the Cyber Incident Framework is designed to operationalize cyber resilience: governance, identify, protect, detect, respond, and recover<sup>16</sup>. Moreover, the European Union's Digital Operational Resilience Act (**DORA**) mandates all financial entities to submit an initial notification, an intermediary or interim report and a significant report<sup>17</sup>. DORA has structured report classification into six quantifiable materiality thresholds, such as financial counterparts affected, operation downtime, geographical spread, data loss, criticality of affected services, and direct economic impacts<sup>18</sup>.

In Cambodia, the Draft Law has emphasized that reporting of cybersecurity incidents is mandatory; it also requires CIIO to notify the Cambodian Cybersecurity Unit (**CCU**) and those affected by the incident as soon as they learn about it. The CII must support the serious incident within 12 to 72 hours and general cyber incidents in the same timeframe. However, the draft law does not define a standard reporting template, a secure transmission portal, or a formal way to escalate between agencies. The Draft Law also requires Critical Information Infrastructures Organization (**CIIOs**) to immediately notify the Cambodian Cybersecurity Unit (**CCU**) and persons affected by the cybersecurity incident from the time when the CIIOs learn of the incident of serious impact and within 12 (twelve) to 72 (seventy-two) hours from the time when the CIIO learns of the general cyber incidents<sup>19</sup>. However, the Draft Law does not define standardized reporting templates, security transmission portals, or a formal inter-agency escalation channel.

## III. Existing Cybersecurity Incident Reporting Landscape in Cambodia

Currently, in Cambodia, there are no laws or regulations that address cybersecurity event notifications or procedures<sup>20</sup>. However, there are relevant laws and regulations with provisions related to cybersecurity issues such as Criminal Code 2009, Law on Telecommunications 2015, Law on Electronic Commerce 2019, Law on Banking and Financial Institutions, 1999, Prakas on Credit Reporting 1999, Law on Anti-Money Laundering and Combating the Financing of Terrorism 2020, The TCRMG 2026, Law on the Management of Private Medical, Paramedical, and Medical Aid Profession, and Medical Aid Profession 2000, Sub-decree on the Code

13 National Institute of Standards and Technology (NIST), “Cybersecurity Incident,” NIST Computer Security Resource Center Glossary, accessed June 19, 2026, [https://csrc.nist.gov/glossary/term/cybersecurity\\_incident](https://csrc.nist.gov/glossary/term/cybersecurity_incident); Australian Signals Directorate, “Guidelines for Cyber Security Incidents,” Cyber.gov.au, last updated June 9, 2026, <https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cyber-security-incidents>;

14 European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape: Finance Sector (January 2023 to June 2024) (2024), pp. 10. 6-7. [https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024\\_Final.pdf](https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf).

15 CyberCX, Cambodian Cyber Security Capability Assessment, prepared on behalf of the Cambodian Government and supported by the Australian Department of Foreign Affairs and Trade, version 1.0 (April 2022), pp. 8-9, 60, [https://cadf.edu.kh/wp-content/uploads/2024/06/Cambodian\\_Cyber\\_Security\\_Capability\\_Assessment\\_v1\\_0\\_04\\_04\\_22\\_DRAFT.pdf](https://cadf.edu.kh/wp-content/uploads/2024/06/Cambodian_Cyber_Security_Capability_Assessment_v1_0_04_04_22_DRAFT.pdf).

16 National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 (February 26, 2024), p. 3. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.

17 European Supervisory Authorities (EBA, EIOPA, and ESMA), Final Report on the Draft Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) on Incident Reporting (JC 2024-33) (Paris: ESMA, July 17, 2024), p. 5. [https://www.esma.europa.eu/sites/default/files/2024-07/JC\\_2024-33\\_-\\_Final\\_report\\_on\\_the\\_draft\\_RTS\\_and\\_ITS\\_on\\_incident\\_reporting.pdf](https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf).

18 European Supervisory Authorities (EBA, EIOPA, and ESMA), Final Report on the Draft Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) on Incident Reporting (JC 2024-33) (Paris: ESMA, July 17, 2024), p. 38.

19 Professor Phallack Kong, “Designing a Cybersecurity Legal Framework for Cambodia,” in Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond, ed. Phallack Kong and Thomas Honnet (Phnom Penh: Konrad-Adenauer-Stiftung Cambodia, 2023), pp. 109.

20 Lim Chong Kin and David N. Alfred, eds., DNA ASEAN Guide to Data Protection and Cybersecurity Regulation in Southeast Asia 2025 (Bangkok: Tilleke & Gibbins, 2025), pp. 34, <https://www.tilleke.com/wp-content/uploads/2025/12/DNA-ASEAN-Guide-to-Data-Protection-and-Cybersecurity-Regulation-in-Southeast-Asia-2025.pdf>



of Medical Ethics 2016<sup>21</sup>, and most recently, Cambodia enacted a new law on Combating Technological Fraud. All those laws have established mechanisms of data breach or automated incident reporting as mandatory, and the last law focuses on criminal enforcement rather than proactive organizational cyber resilience<sup>22</sup>.

To address this gap, Cambodia has proposed a legal framework on cybersecurity. The Draft Law has provided the competent authority for national cybersecurity management, served by the National Computer Emergency Response Team (National CERT) and operating the central cybersecurity control operation system<sup>23</sup>. The Draft Law has classified the banking and finance sector as an essential service, scoping both public and private institutions, and created a legal mandate to create a unit in charge of cybersecurity, develop internal regulations on cybersecurity management, evaluate cybersecurity risks, mitigate risk, notify incidents, and cooperate with ministries/institutions and relevant stakeholders to manage cybersecurity tasks<sup>24</sup>.

Simultaneously, NBC has published its own comprehensive TCRMG. This guide aims to enable BFIs to establish a robust technology risk management framework, to strengthen cybersecurity resilience, and ensure the safety, security and efficiency of their operations while fostering stable growth and protecting customers<sup>25</sup>. The TCRMG has a strict internal incident management process, including defined staff roles, severity classification scales, and post-mortem analyses<sup>26</sup>. As evidence of enforcement under the guidelines, on November 27, 2021, NBC issued a circular enforcing the TCRMG 2019, requiring BFIs to resolve technical problems within 2 hours<sup>27</sup>. In 2026, NBC launched a new TCRMG that requires BFIs to report incidents periodically or on an ad hoc basis and immediate reporting for any operational interruptions affecting mobile banking applications or electronic payment networks<sup>28</sup>.

This dual-track regulatory structure creates a direct overlap between the Cybersecurity Authority's centralized mandate and the NBC's sectoral authority.

**Table 1: Regulatory Overlap and Structural Friction in Cambodia's Incident Reporting**

| Dimensions                       | Cybersecurity Draft Law                                         | NBC Guideline                                  |
|----------------------------------|-----------------------------------------------------------------|------------------------------------------------|
| Primary Regulatory Authority     | Ministry of Post and Telecommunications <sup>29</sup>           | National Bank of Cambodia <sup>30</sup>        |
| Legal Status of Banking Entities | Critical Information Infrastructure Organizations <sup>31</sup> | Banks and Financial Institutions <sup>32</sup> |

21 Sang Sinawong et al., "Cybersecurity Legislation: Policy Instrument to Improve Cybersecurity Readiness and Resilience," in Cambodia in Cyberspace: Anthology, ed. Siriwat Chhem, Ou Phannarith, and Chea Vatana (Phnom Penh: Asian Vision Institute, 2022), p. 98, <https://asianvision.org/wp-content/uploads/2023/05/Cambodia-in-Cyberspace-Anthology.pdf>  
Cambodia, Office of the Council of Ministers, "Regarding the Most Esteemed Recommendations of Samdech Thipadei Prime Minister... Journey Towards Digital Transformation and Future Directions of the Ministry of Post and Telecommunications," Notification No. 265 SCN.PB, Unofficial English Translation (Phnom Penh, February 18, 2025), accessed May 20, 2026, <https://asset.cambodia.gov.kh/mpmc/2025/06/20250218-SCN-265-ENG-FINAL.pdf>; Tilleke & Gibbins, Cybersecurity and Data Protection in Mainland Southeast Asia 2024, legal industry report (Tilleke & Gibbins, July 2024), pp. 1-6, accessed May 20, 2026, <https://www.tilleke.com/wp-content/uploads/2024/07/Tilleke-Cybersecurity-and-Data-Protection-in-Mainland-South-east-Asia-2024.pdf>; Open Development Cambodia, "Cybersecurity in Cambodia: Current Developments and Challenges Ahead," policy briefing repository, accessed May 20, 2026, [https://data.opendatacambodia.net/en/dataset/e4d6510e-2244-445b-82ac-2007532742ab/resource/2c3017d5-2b6a-4b12-9f2a-12244563a3f1/download/cybersecurity\\_in\\_cambodia\\_current\\_developments\\_and\\_challenges\\_ahead.pdf](https://data.opendatacambodia.net/en/dataset/e4d6510e-2244-445b-82ac-2007532742ab/resource/2c3017d5-2b6a-4b12-9f2a-12244563a3f1/download/cybersecurity_in_cambodia_current_developments_and_challenges_ahead.pdf).

22 Reuters, "Cambodian Parliament Passes Landmark Cybercrime Law After Scam Centre Scrutiny," Reuters, April 4, 2026, <https://www.reuters.com/world/asia-pacific/cambodian-parliament-passes-landmark-cybercrime-law-after-scam-centre-scrutiny-2026-04-03/>.

23 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 117.

24 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," op. cit., p. 118.

25 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026 (Phnom Penh: National Bank of Cambodia, 2026), p. 2.

26 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026, op. cit., p. 11.

27 National Bank of Cambodia, Notification No. BK. 07.019.575 on the Implementation of the Guidelines on Information Technology Risk Management (Phnom Penh: NBC, July 22, 2019), para. 2. See also Michael Firn, "NBC Says It Will Take Procedural Action After ABA Outage," Khmer Times, November 26, 2021, <https://www.khmertimeskh.com/50978132/nbc-says-it-will-take-procedural-action-after-aba-outage/>.

28 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026 (Phnom Penh: National Bank of Cambodia, 2026), p. 12.

29 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 106.

30 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (2026), Introduction, p. 2.

31 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 107-108.

32 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (2026), Abbreviation, p. 1.

|                                    |                                                                                                                     |                                                                                   |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Core Reporting Triggers            | Cybersecurity incidents affecting cybersecurity management systems <sup>33</sup>                                    | IT incidents affecting systems, data, payment rails, or mobile apps <sup>34</sup> |
| Initial Notification Window        | Immediate action for incidents of serious impact <sup>35</sup> 12 to 72 hours for all other incidents <sup>36</sup> | Report incidents periodically or on an ad hoc basis <sup>37</sup>                 |
| Statutory Non-Compliance Penalties | Criminal liability for legal entities <sup>39</sup>                                                                 | Procedural regulatory actions <sup>38</sup>                                       |

## IV. Comparative International Approaches to Cybersecurity Incident Reporting

This section provides a comparative analysis of global cybersecurity governance frameworks that balance centralized national security with sector-specific supervision.

**Table 2: Comparative Global Approaches to Cybersecurity Incident Reporting**

| Jurisdiction / Framework                                        | Lead Regulatory Body                                    | Primary Initial Timeline                         | Supplemental / Final Deadlines                                                | Treatment of Third-Party & Cloud Risks                                                                 | Sector-Central Coordination Model                                                                                                  |
|-----------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Digital Operational Resilience for the Financial Sector (DO RA) | EU Supervisory Authority/National Financial Supervisors | Major 4 hours after classification <sup>40</sup> | 72 hours (Intermediate) <sup>41</sup><br>1 month (Final Report) <sup>42</sup> | Regulates ICT third-party providers as direct supervisory targets <sup>43</sup> 1 month (Final Report) | Sector-first: BFs report to the financial supervisor; supervisor alerts the Computer Security Incident Response Team <sup>44</sup> |
| Singapore Cybersecurity Act                                     | Cyber Security Agency (CSA) <sup>45</sup>               | Max 2 hours from awareness for CII <sup>46</sup> | 72 hours (Supplement) <sup>47</sup><br>30 days (Final Report) <sup>48</sup>   | Extends direct regulatory oversight to third-party-owned infrastructure <sup>49</sup>                  | Dual-reporting using aligned, single-submission flows                                                                              |

33 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 109.

34 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (2026), ch. 3.8.0.

35 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 109.

36 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 109.

37 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (2026), ch. 3.8.9.

38 Firn, "NBC Says It Will Take Procedural Action," Khmer Times, 2021.

39 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 110.

40 Matthieu Roland, "DORA RTS & ITS: Complete Regulatory Technical Standards Reference 2026," Regulation-Dora.EU, January 17, 2025, arts. 18(3), 19(1), <https://www.regulation-dora.eu/rts>

41 Matthieu Roland, "DORA RTS & ITS: Complete Regulatory Technical Standards Reference 2026," Regulation-Dora.EU, January 17, 2025, arts. 18(3), 19(1), art.18(3).

42 Commission Delegated Regulation (EU) Supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council about regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats, Article 5. [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\\_202500301](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500301)

43 Matthieu Roland, "DORA RTS & ITS: Complete Regulatory Technical Standards Reference 2026," Regulation-Dora.EU, January 17, 2025, art. 30.

44 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) Article 10 -11. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555>

45 "Cybersecurity Act 2018 - Singapore Statutes Online." 2018. Agc.gov.sg. 2018, pt., 5(2).

46 Cybersecurity (Critical Information Infrastructure) Regulations (Singapore), reg. 5(1)(a).

47 Cybersecurity (provider-owned Critical Information Infrastructure) Regulations 2018, etc. 5. 2(C). <https://sso.agc.gov.sg/SL/CA2018-S519-2018?DocDate=20251015>

48 Cybersecurity (provider-owned Critical Information Infrastructure) opt cit., Regulations 2018, etc. 5. 2(C).

49 Cybersecurity (provider-owned Critical Information Infrastructure), opt cit., Section 14(1)(b), (ba), (bb).

|                                                              |                                                                     |                                                                                                |                                                                        |                                                                         |                                                                                                      |
|--------------------------------------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| USA Cyber Incident Reporting for Critical Infrastructure Act | Cybersecurity & Infrastructure Security Agency (CISA) <sup>50</sup> | 72 hours (substantial incidents) <sup>51</sup><br><br>24 hours (ransom payments) <sup>52</sup> | Promptly submit supplemental reports as new data emerges <sup>53</sup> | Focuses on systemic supply chain targets and critical service providers | Centralized Clearinghouse: Reports go to CISA; CISA coordinates with sector regulators <sup>54</sup> |
|--------------------------------------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|

## V. Developing a Cybersecurity Incident Reporting Framework for Cambodia's Banking Industry

Based on the international practice, Cambodia should create a reporting model in favor of a sector-first, nationally coordinated approach. In this regard, bypassing NBC's supervisory structure would ignore its deep expertise in financial system operations<sup>55</sup>. As the custodian of system stability, NBC is uniquely positioned to assess how a cyber disruption would affect payment transactions, liquidity flows, and customer trust. In the initial report case, NBC shall immediately coordinate with MPTC's National CERT to ensure technical threat intelligence is rapidly integrated into national cyber situational awareness and cross-sector defense<sup>56</sup>. In case of a serious incident that threatens national security or financial stability, the report should be made immediately to the Digital Security Committee (**DSC**), to preserve NBC's sector-specific expertise while strengthening centralized national security coordination<sup>57</sup>.

To operationalize this model, Cambodia should establish three core structural pillars:

### 1. Aligned Incident Classification Standards

Cambodia should align the incident severity definitions defined by MPTC and NBC into a single standard, based on DORA practice. Incidents should be categorised into three layers:

- **Critical Incidents:** Incidents causing total disruption to critical payment networks, major data breaches exposing banking databases, and ransomware attacks locking down core banking systems<sup>58</sup>.
- **Major Incidents:** Incidents causing localised service degradation or physical security breaches. These require prompt containment and must be reported within a 12-to-24-hour window<sup>59</sup>.
- **Minor Incidents:** Incidents such as standard phishing attempts, misconfigurations, or failed backup processes with zero operational impact. These should be logged internally and reported to the NBC in consolidated quarterly updates, rather than triggering urgent national workflows<sup>60</sup>.

50 H. R. 2471-1006, SEC. 104. FEDERAL SHARING OF INCIDENT REPORTS.

51 "SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS. H. R. 2471-995. <https://www.govinfo.gov/content/pkg/BILLS-117hr2471enr/pdf/BILLS-117hr2471enr.pdf>

52 "SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS. H. R. opt cit., 2471-995.

53 "SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS. H. R. opt cit., 2471-995.

54 H. R. 2471-1006, SEC. 104. FEDERAL SHARING OF INCIDENT REPORTS.

55 Financial Stability Board, Achieving Greater Convergence in Cyber Incident Reporting: Consultative Document (October 17, 2022), p. 36, <https://www.fsb.org/uploads/P171022.pdf>

56 Financial Stability Board, Achieving Greater Convergence in Cyber Incident Reporting: Consultative Document (October 17, 2022), p. 17, Recommendation 10, <https://www.fsb.org/uploads/P171022.pdf>

57 Professor Phallack Kong, "Designing a Cybersecurity Legal Framework for Cambodia," p. 106-107

58 REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, Article 19. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554>; National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026 (Phnom Penh: National Bank of Cambodia, 2026), p. 54.

59 REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, Article 19. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554>; National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026 (Phnom Penh: National Bank of Cambodia, 2026), p. 54.

60 National Bank of Cambodia, Technology and Cyber Risk Management Guidelines (TCRMG) 2026 (Phnom Penh: National Bank of Cambodia, 2026), p. 54.

## 2. Standardised, Phased Reporting Obligations

Cambodia should replace its single, ambiguous “immediate” reporting requirement with a structured, three-phase notification process:

- **Phase 1 Initial Notification (4 Hours):** Concentrate on alerting the NBC and MPTC of the ongoing incident to know the facts such as the date and time of detection, the nature of the attack, and preliminary containment measures<sup>61</sup>.
- **Phase 2 Intermediate Report (72 Hours):** Submitted when the initial investigation is underway. This report shall consist of updated impact metrics, affected technical assets, and the estimated recovery timeline<sup>62</sup>.
- **Phase 3 Final Report (30 Days):** In this stage, the report should be a comprehensive post-incident document that identifies the cause of the incident, forensic evidence, lessons learned and a documented long-term remediation plan<sup>63</sup>.

## 3. Integrated, Secure Operational Reporting Infrastructure

To ensure protection of sensitive personal data based on international practice, Cambodia should develop secure operational reporting tools. MPTC and NBC should co-develop a centralized, encrypted incident reporting portal. This secure infrastructure must incorporate:

- Encrypted communication channels, Secure Sockets Layer (**SSL**), Transport Layer Security (**TLS**) and end-to-end Pretty Good Privacy Protocols to prevent interception of sensitive reports<sup>64</sup>.
- Multi-factor authentication (MFA) to restrict access to authorized personnel<sup>65</sup>.
- Automated incident reference codes to track incidents across their lifecycle<sup>66</sup>, and
- Standardized, machine-readable reporting templates to allow rapid data aggregation and cross-sector threat correlation<sup>67</sup>.

61 Matthieu Roland, “DORA RTS & ITS: Complete Regulatory Technical Standards Reference 2026,” Regulation-Dora.eu, January 17, 2025, arts. 18(3), 19(1).

62 Supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats, Article 5. [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\\_202500301](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500301)

63 Supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats, Article 5. [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\\_202500301](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500301)

64 National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, rev. 5 (September 2020), pp. 204-306, Control SC-8 (Transmission Confidentiality and Integrity); <https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-53r5.pdf>; ISO IEC 27002 Information security, cybersecurity and privacy protection-Information security controls, page 115.

65 NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management, Section 4 (Authenticator Assurance Level 2 - AAL2), page 3. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf> ISO IEC 27002 Information security, cybersecurity and privacy protection-Information security controls, Control 5.17 (Authentication Information), page 31; National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, rev. 5 (September 2020), Control IA-2(1) (Multi-Factor Authentication to Privileged Accounts) pp.,132.

66 Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. 2012. “Computer Security Incident Handling Guide.” Computer Security Incident Handling Guide 2 (2), Section 3.2.5 Incident Documentation, Page 30-31, [nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf)

67 Jordan, Bret, Rich Piazza, John Wunder, and Bret Latest. 2021. “This Specification Replaces or Supersedes: •STIX Version 2.0. Part 1: STIX Core Concepts. Edited • STIX Version 2.0. Part 2: STIX Objects. Edited.”, Page 2, <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.pdf>; (“Format for Incident Reporting Exchange (FIRE)” n.d.), Page 2, 3, 6 <https://www.fsb.org/uploads/P150425-1.pdf>

## VI. Conclusion

Cambodia is moving toward an integrated digital economy, financial innovation and growth, but concurrently creating critical cybersecurity dependencies. The banking and financial sector is increasingly adopting emerging technologies like real-time payment systems, distributed ledgers, and artificial intelligence; all this toll is potentially impacting a major systemic cyber disruption that grows exponentially. The proactive approach to building resilient and highly coordinated cybersecurity governance is no longer just a technical operational goal; it is a necessity for national economic stability, national security, and public trust.

While both the NBC's 2026 TCRMG and the MPTC's Draft Law on Cybersecurity represent major milestones in Cambodia's legal development, their lack of structural alignment presents a significant governance challenge. Overlapping mandates, conflicting incident reporting timelines, and ambiguous escalation paths risk diverting critical resources during a cyber crisis. By adopting the "sector-first, nationally coordinated" model proposed in this law brief, Cambodia can successfully harmonise its regulatory architecture. This framework leverages the NBC's deep financial and macroprudential expertise while building a unified national cyber defence led by the MPTC and National CERT.



## Bibliography

### Legislation

1. Cambodia. Criminal Code 2009.
2. Cambodia. Law on Anti-Money Laundering and Combating the Financing of Terrorism 2020.
3. Cambodia. Law on Banking and Financial Institutions 1999.
4. Cambodia. Law on Combating Technological Fraud 2026.
5. Cambodia. Law on Electronic Commerce 2019.
6. Cambodia. Law on Telecommunications 2015.
7. Cambodia. Law on the Management of Private Medical, Paramedical, and Medical Aid Profession, and Medical Aid Profession 2000.
8. Republic of Singapore. Cybersecurity (Amendment) Act 2024. Singapore: AGC, 2024.
9. United States Congress. Consolidated Appropriations Act, 2022. H.R. 2471. 117th Congress. Government Publishing Office, 2022.

### Guidelines / Regulations

1. Cambodia. Prakas on Credit Reporting 1999.
2. Cambodia. Sub-decree on the Code of Medical Ethics 2016.
3. National Bank of Cambodia. *Technology and Cyber Risk Management Guidelines (TCRMG)* 2026. Phnom Penh: National Bank of Cambodia, 2026.
4. National Bank of Cambodia. Notification No. BK. 07.019.575 on the Implementation of the Guidelines on Information Technology Risk Management. Phnom Penh: NBC, July 22, 2019.
5. National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. February 26, 2024. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
6. Roland, Matthieu. "DORA RTS & ITS: Complete Regulatory Technical Standards Reference 2026." *Regulation-Dora.eu*, DORA Regulation EU, 17 Jan. 2025
7. Supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats.
8. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
9. Cybersecurity Critical Information Infrastructure Regulations (Singapore).
10. European Union. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial Financial Stability Board. Achieving Greater Convergence in Cyber Incident Reporting: Consultative Document. 2022.sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554>
11. European Union. Commission Delegated Regulation (EU) Supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats. [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L\\_202500301](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500301)
12. Cyber Security Coalition. Cyber Security Incident Management Guide. [https://cybersecuritycoalition.be/wp-content/uploads/cybersecurity-incident-management-guide\\_EN.pdf](https://cybersecuritycoalition.be/wp-content/uploads/cybersecurity-incident-management-guide_EN.pdf)

### Official Reports / Government Policy Documents

1. Royal Government of Cambodia. *Pentagonal Strategy Phase I: For Growth, Employment, Equity, Efficiency and Sustainability*. Phnom Penh: Council of Ministers, August 2023.
2. Royal Government of Cambodia / National Bank of Cambodia. *Cambodia Financial Technology Development Policy 2023-2028*. (Please replace the local file path with a permanent URL for final submission).
3. Supreme National Economic Council. *Cambodia Digital Economy and Society Policy Framework 2021-2035*. Phnom Penh: RGC, 2021. <https://www.mptc.gov.kh/wp-content/uploads/2021/06/Cambodia-Digital-Economy-and-Society-Policy-Framework-2021-2035.pdf>

4. Ministry of Post and Telecommunications. *Digital Government Policy 2022-2035*. Phnom Penh: MPTC, 2022. <https://mptc.gov.kh/wp-content/uploads/2022/03/Digital-Government-Policy-2022-2035-EN.pdf>
5. National Bank of Cambodia. *Financial Stability Report 2025*. Phnom Penh: National Bank of Cambodia. [https://www.nbc.gov.kh/download\\_files/publication/fsr\\_eng/FSR2025\\_En.pdf](https://www.nbc.gov.kh/download_files/publication/fsr_eng/FSR2025_En.pdf)
6. World Bank Forum. *Global Cybersecurity Outlook 2026*. Insight Report.
7. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape: Finance Sector (January 2023 to June 2024)*. 2024. [https://www.enisa.europa.eu/sites/default/files/202502/Finance%20TL%202024\\_Final.pdf](https://www.enisa.europa.eu/sites/default/files/202502/Finance%20TL%202024_Final.pdf)
8. European Supervisory Authorities (EBA, EIOPA, and ESMA). *Final Report on the Draft Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) on Incident Reporting (JC 2024-33)*. Paris: ESMA, July 17, 2024. [https://www.esma.europa.eu/sites/default/files/2024-07/JC\\_2024-33\\_-\\_Final\\_report\\_on\\_the\\_draft\\_RTS\\_and\\_ITS\\_on\\_incident\\_reporting.pdf](https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf)
9. Australia, Australian Signals Directorate. *Guidelines for Cyber Security Incidents*. [Cyber.gov.au](https://www.cyber.gov.au/sites/default/files/2026-06/04.%20ISM%20-%20Guidelines%20for%20cyber%20security%20incidents%20%28June%202026%29.pdf). Last updated June 9, 2026. <https://www.cyber.gov.au/sites/default/files/2026-06/04.%20ISM%20-%20Guidelines%20for%20cyber%20security%20incidents%20%28June%202026%29.pdf>
10. Cambodia, Office of the Council of Ministers. "Regarding the Most Esteemed Recommendations of Samdech Thipadei Prime Minister... Journey Towards Digital Transformation and Future Directions of the Ministry of Post and Telecommunications." Notification No. 265 SCN.PB. Unofficial English Translation. Phnom Penh, February 18, 2025. <https://asset.cambodia.gov.kh/mptc/2025/06/20250218-SCN-265-ENG-FINAL.pdf>
11. Tilleke & Gibbins. *Cybersecurity and Data Protection in Mainland Southeast Asia 2024*. Legal industry report. July 2024. <https://www.tilleke.com/wp-content/uploads/2024/07/Tilleke-Cybersecurity-and-Data-Protection-in-Mainland-Southeast-Asia-2024.pdf>
12. Access Now. *Legal Analysis of Cambodia's Draft Cybersecurity Law*. September 29, 2023. <https://www.accessnow.org/wp-content/uploads/2023/10/Legal-Analysis-Cambodia-Cybersecurity-Draft-Law-Final-29-Sept.pdf>
13. Open Development Cambodia. *Cybersecurity in Cambodia: Current Developments and Challenges Ahead*. Policy briefing repository. [https://data.opendevdevelopmentcambodia.net/en/dataset/e4d6510e-2244-445b-82ac-2007532742ab/resource/2c3017d5-2b6a-4b12-9f2a-12244563a3f1/download/cybersecurity\\_in\\_cambodia\\_current\\_developments\\_and\\_challenges\\_ahead.pdf](https://data.opendevdevelopmentcambodia.net/en/dataset/e4d6510e-2244-445b-82ac-2007532742ab/resource/2c3017d5-2b6a-4b12-9f2a-12244563a3f1/download/cybersecurity_in_cambodia_current_developments_and_challenges_ahead.pdf)
14. CyberCX. *Cambodian Cyber Security Capability Assessment*. Prepared on behalf of the Cambodian Government and supported by the Australian Department of Foreign Affairs and Trade, version 1.0, April 2022. [https://cadf.edu.kh/wp-content/uploads/2024/06/Cambodian\\_Cyber\\_Security\\_Capability\\_Assessment\\_v1\\_0\\_04\\_04\\_22\\_DRAFT.pdf](https://cadf.edu.kh/wp-content/uploads/2024/06/Cambodian_Cyber_Security_Capability_Assessment_v1_0_04_04_22_DRAFT.pdf)
15. World Bank Forum. *Global Cybersecurity Outlook 2026*. Insight Report. 2026. [https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/cybersecurity-and-geopolitical-risks-in-financial-markets\\_e7efd32a/1002b1fd-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/cybersecurity-and-geopolitical-risks-in-financial-markets_e7efd32a/1002b1fd-en.pdf)
16. Financial Stability Board. *Achieving Greater Convergence in Cyber Incident Reporting: Consultative Document*. 2022. <https://www.fsb.org/uploads/P171022.pdf>

## Books

1. Hoofnagle, Chris Jay, and Golden G. Richard III. *Cybersecurity in Context: Technology, Policy, and Law*. Hoboken, NJ: Wiley, 2025.

## Book Chapters

1. Professor Kong, Phallack. "Designing a Cybersecurity Legal Framework for Cambodia." In *Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond*, edited by Phallack Kong and Thomas Honnet, 104-118. Phnom Penh: Konrad-Adenauer-Stiftung Cambodia, 2023.
2. Sang, Sinawong, Phallack Kong, Phannarith Ou, and Siriwat Chhem. "Cybersecurity Legislation: Policy Instrument to Improve Cybersecurity Readiness and Resilience." In *Cambodia in Cyberspace: Anthology*, edited by Siriwat Chhem, Phannarith Ou, and Vatana Chea, 97. Phnom Penh: Asian Vision Institute, 2022.

## Security In Standards

1. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Rev. 2. Gaithersburg, MD: National Institute of Standards and Technology, 2012.
2. European Commission. Supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council about Regulatory Technical Standards Specifying the Content and Time Limits for the Initial Notification of, and Intermediate and Final Report on, Major ICT-Related Incidents, and the Content of the Voluntary Notification for Significant Cyber Threats. Article 5. 2025.
3. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Rev. 5. Gaithersburg, MD: NIST, September 2020.
4. National Institute of Standards and Technology. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B. Gaithersburg, MD: NIST.
5. OASIS Open. STIX™ Version 2.1: Structured Threat Information Expression. Edited by Bret Jordan, Rich Piazza, John Wunder, et al. 2021.
6. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, rev. 5, 2020.
7. Financial Stability Board. Format for Incident Reporting Exchange (FIRE). n.d.
8. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27002: Information Security, Cybersecurity and Privacy Protection-Information Security Controls. Geneva: ISO/IEC.

## News Articles

1. Firn, Michael. "NBC Says It Will Take Procedural Action After ABA Outage." Khmer Times, November 26, 2021. <https://www.khmertimeskh.com/50978132/nbc-says-it-will-take-procedural-action-after-aba-outage/>
2. Roland, Matthieu. "DORA RTS & ITS: Complete Regulatory Technical Standards Reference 2026." Regulation-Dora.eu. January 17, 2025. <https://www.regulation-dora.eu/>.

## Web Sources / Other

1. National Institute of Standards and Technology (NIST). "Cybersecurity Incident." NIST Computer Security Resource Center Glossary. [https://csrc.nist.gov/glossary/term/cybersecurity\\_incident](https://csrc.nist.gov/glossary/term/cybersecurity_incident)
2. CISO Marketplace. "2026 Compliance Countdown: New Cybersecurity Regulations CISOs Must Know." CISO Marketplace Blog. <https://cisomarketplace.com/blog/2026-compliance-countdown-new-cybersecurity-regulations-cisos-must-know>
3. SearchInform. Incident Lifecycle Management: An In-depth Guide. <https://searchinform.com/articles/cybersecurity/measures/incident-response/incident-lifecycle/>
4. National Bank of Cambodia. Technology and Cyber Risk Management Guidelines Summary - TCRMG (Video Explainer). Phnom Penh, May 2026.
5. ASEAN. ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace. 2025. [https://asean.org/wp-content/uploads/2025/02/ASEAN\\_checklist\\_print.pdf](https://asean.org/wp-content/uploads/2025/02/ASEAN_checklist_print.pdf).



**PART III  
GREEN FINANCE  
AND DIGITAL FINANCIAL LAW**





## Carbon Credit Trading in Cambodia

*POENG Somalika*



## Abstract

On January 9, 2024, Cambodia has launched its Article 6 Operations Manual and officially launched its national carbon registry on October 31 2025, the recent updated still omitting a clear definition and legal status of a carbon credit. Without clear statutory classification, can lead to significant problems. In the event of a dispute, no court can determine (i) in the case that whether a judgment creditor may seize a credit, (ii) whether a bank may accept a credit as pledged collateral, (iii) whether a trading platform requires a securities license, or (iv) whether the government's contractual claim to 10% of credits is enforceable against a third-party purchaser.

This brief discusses three potential classifications under existing Cambodian law: (1) intangible property, (2) securities/derivative instrument, or (3) sui generis. By drawing on the legal frameworks of Indonesia and Malaysia. Those ASEAN members that represent the distinct legal strategies available to a civil-law developing country. Indonesia treats carbon as securities under its Financial Services Authority (OJK) Regulation No. 14/2023<sup>1</sup>; while Malaysia operates a voluntary carbon exchange (Bursa Carbon Exchange) alongside a forthcoming compliance market<sup>2</sup>.

This brief recommends that Cambodia enact dedicated legislation explicitly defining carbon credits as regulated intangible assets subject to dual oversight by the Ministry of Environment (“MOE”) and the Securities and Exchange Regulator of Cambodia (“SERC”).

## I. Introduction

A carbon credit is a tradable unit representing one metric tonne of carbon dioxide equivalent (1 tCO<sub>2</sub>e) reduced or removed through projects such as Reducing Emissions from Deforestation and Forest Degradation (REDD+)<sup>3</sup>.

On 09 January 2024, the MOE officially launched the Operations Manual for the Implementation of Article 6 of the Paris Agreement on Climate Change in Cambodia (“**Article 6 Operations Manual**”) referenced to the formal authorization from Royal Government of Cambodia (“**RGC**”<sup>4</sup>). As stated in Article 6 Operation Manual, Cambodia issues two types of units: (i) Internationally Transferred Mitigation Outcomes (“**ITMOs**”) authorized for international transfer toward another country's Nationally Determined Contribution (“**NDC**”<sup>5</sup>) ; and (ii) Greenhouse Gas Emission Reductions (“**GHG ERs**”<sup>6</sup>). These broader category of verified emission reductions (VERs). The credits that generated by project proponents, verified by accredited third parties such as Verra or Gold Standard, and recorded in the registries. This was followed by the establishment of the Cambodia Carbon Registry (“**CCR**”) under the supervision of MOE in 2025<sup>7</sup>. These frameworks only able to provide detailed administrative rules for the authorization, issuance, and tracking ITMOs and GHG ERs<sup>8</sup>.

This brief will narrow its focus to a specific legal question that remains unanswered: which existing legal category would a court use to classify a carbon credit, and what practical consequences would follow from each possible classification, and which legal reasoning in the classification may appear more exceptional and why? The current stakes are substantial, currently hundreds of millions of dollars anticipated from carbon credit projects including Green Carbon Inc.'s planned 20 million tonnes of CO<sub>2</sub> reductions over 500,000 hectares may rest on legally unstable ground. We will examine whether carbon credits constitute as intangible property, securities or derivative instrument, or a sui generis asset under existing Cambodian legislation, together with an analysis of the legal validity of each classification.

---

1 Otoritas Jasa Keuangan [Financial Services Authority], Regulation of the Financial Services Authority of the Republic of Indonesia Number 14 of 2023 concerning Carbon Trading through Carbon Exchanges, issued August 2, 2023

2 Bursa Malaysia, “*Bursa Malaysia Launches a Voluntary Carbon Market Exchange*,” December 9, 2022, [https://www.bursa-malaysia.com/bm/about\\_bursa/media\\_centre/bursa-malaysia-launches-a-voluntary-carbon-market-exchange](https://www.bursa-malaysia.com/bm/about_bursa/media_centre/bursa-malaysia-launches-a-voluntary-carbon-market-exchange).

3 Article 6 of Operational Manual, p.8

4 Letter No. 1380 Sor Chor Nor. Dor Bor dated 14 December 2023, issued by Office of Council of Ministers

5 Article 6 of Operational Manual, p.iii

6 *Ibid.*

7 “*Environment Ministry Launches Carbon Registry for Transparency, Accountability*,” Khmer Times, October 11, 2024, <https://www.khmertimeskh.com/501782990/environment-ministry-launches-carbon-registry-for-transparency-accountability/>.

8 Article 6 of Operations Manual, p. 8; Cambodia Carbon Registry, “How It Works,” MOE, <https://ccr.gov.kh/how-it-works>.

## II. Legal Classification under existing Cambodian Law

The primary issue concerning the absence of the legal classification of carbon credits under Cambodian Law. Unless there is a clear determination of what is legal definition of carbon credits and legal nature of carbon credits, the secondary issues concerning ownership, transfer, enforcement, licensing, etc. will remain uncertain. This constitutes both a gap in the existing legal framework and the interpretation of broad legal concepts. Additionally, this may also create conflicts of law between different areas of Cambodia Law where more than one legal category could potentially apply.

Carbon credits can be classified by using the core determinants such as its (1) market mechanism under which the carbon credits are developed and traded; and (2) trading models through which the credit is recorded and transferred. Though, these determinants do not automatically establish the legal classification of a carbon credit. Rather, they assist in identify the rights attached to the credit and the legal rules that may potentially apply.

### 2.1. Market Mechanisms

The legal classification of a carbon credit depends significantly on the regulatory or contractual framework governing its creation, issuance, transfer, and retirement. Likewise, Carbon credits cannot be assessed merely in the abstract, because their legal characteristics may vary according to the market in which they operate and the rules governing their transfer. There are two types of carbon market mechanism (A) Mandatory (Compliance) Market; and (B) Voluntary Carbon Market.

#### A. Mandatory (Compliance) Market

In compliance market, regulated entities must meet emission reduction targets set by the governments<sup>9</sup>. The right and obligation to reduce or account for emissions is therefore legally binding rather than voluntary. Two common regulatory mechanisms are:

1. Emissions Trading System (ETS): such as European Union ETS, under which governments set emission caps for companies and issue or auction emission allowance upfront to regulated entities<sup>10</sup>; or
2. Carbon Taxes Systems: where governments set a fixed price on CO<sub>2</sub> emitted on a specified quantity of GHGs<sup>11</sup>.

It is noteworthy that these two mechanisms should not be treated as legally identical, as ETS generally creates tradable regulatory units, whereas a carbon tax primarily imposes a financial obligation and does not necessarily create a transferable carbon asset.

Carbon units operating in compliance market are typically recognized as statutory or regulatory instrument because their creation, issuance, transfer, and cancellation are governed by legislation or administrative regulation. Thus, it comes to enforceability it is much clearer as they are embedded in public law.

#### B. Voluntary Market

By contract, the Voluntary Carbon Market ("VCM"), businesses and individuals purchase credits voluntarily to offset emissions outside regulatory requirement<sup>12</sup>. Purchasing carbon credits here are solely rely on private contracts, verification bodies, third-party standards, project documents and private carbon registries. The legal rights of market participants therefore depend heavily on the terms of their agreements and the operational rules of the relevant registry or standard requirements body. However, it would be too broad to

9 United Nations Development Programme, "What Are Carbon Markets and How Do They Work?," Climate Promise, May 18, 2022, <https://climatepromise.undp.org/news-and-stories/what-are-carbon-markets-and-how-do-they-work>.

10 European Commission, EU ETS Handbook (Brussels: Directorate-General for Climate Action, 2015), p.4, [https://climate.ec.europa.eu/system/files/2017-03/ets\\_handbook\\_en.pdf](https://climate.ec.europa.eu/system/files/2017-03/ets_handbook_en.pdf).

11 EcoVadis Editorial Team, "Carbon Tax: Understanding Supply Chain Cost Exposure," EcoVadis Blog, June 23, 2026, <https://ecovadis.com/blog/carbon-tax/>.

12 Jing-Li Fan et al., "Global Carbon Market: A Review of the Current Status, Challenges, and Future Prospects," Environmental Science and Ecotechnology 21 (September 2024): 100412, section 3.1, <https://doi.org/10.1016/j.ese.2024.100412>.

state that VCM carbon credits are not legally recognised assets<sup>13</sup>. Their legal status differs between jurisdictions and may depend on the applicable rules of property law, contract law, commercial law, insolvency law, securities regulation, and taxation.

The issues that Cambodia is currently facing is that whether the existing legislation does not clearly determine whether carbon credits constitute: an independently transferable intangible asset; a contractual right enforceable only against specific parties; a financial or investment; a beneficial interest recorded in a private registry; or whether it is another form of legally recognised right. The controversy surrounding the Kariba REDD+ in 2023, where Verra the world's largest carbon credit registry admitted to issuing 15 million excess credits from a forest project known as Kariba REDD+ Project in Zimbabwe<sup>14</sup>. Together Volkswagen, Nespresso, and TotalEnergies had retired over 1.5 million of those credits to certify their products as "carbon neutral"<sup>15</sup>.

Despite the over excess retired credits a registry continues to recognise retired credits as valid, this does not necessarily resolve questions concerning legal ownership, contractual liability, financial loss, or the environmental credibility of the credits. In the absence of a statutory framework, affected parties may have to rely on private-law remedies, including breach of contract, misrepresentation, breach of warranty, negligence, or unjust enrichment. The availability of such remedies will depend on the terms of the contract, the governing law, dispute-resolution clauses, and the identity of the party against whom the claim is brought.

For Cambodia, the VCM therefore raises interconnected issues involving a gap in the law, regulatory implementation, and conflict of laws. A Cambodian project may generate credits under an international standard, record them in a foreign registry, and sell them to an overseas purchaser through a contract governed by foreign law. A dispute may consequently involve Cambodian land and natural resources, a foreign registry, an international certification body, a foreign purchaser, and several potentially applicable legal systems. Determining which law governs ownership and transfer may therefore be as important as determining the substantive classification of the carbon credit.

## 2.2. Trading Models

Carbon credits can be traded in two distinct ways either through (A) Non-Tokenized Trading Model or as (B) Tokenized Trading Model. Each model leads to different issues and if any, the choice between them directly determines which regulatory framework applies as well.

### A. Non-Tokenized Trading Model

Under this trading model, the credits record in a national registry (e.g., CCR). The ownership transfers through two concurrent steps (i) a contractual agreement between the transferor and transferee establishing their respective rights and obligations, and (ii) an amendment to the registry record reflecting the transfer, holding, cancellation, or retirement of the credit<sup>16</sup>. While the registry serves mainly as the administrative record of the transfer and focusing on tracking the ownership and the records transfer history<sup>17</sup>. The primary issue with this model is one of the title and third-party effect. Where a registry is established by statute, legislation may provide that registration constitutes conclusive or prima facie evidence of ownership. This creates a potential loophole regarding title and priority, since the registry entry by itself is administrative rather than statutory, it does not constitute as a proof of legal ownership against third parties.

---

13 International Bar Association, "The Legal Architecture of Carbon Markets: From Global Governance to Corporate Accountability," December 26, 2025, <https://www.ibanet.org/the-legal-architecture-of-carbon-markets-from-global-governance-to-corporate-accountability>

14 Illuminem Editorial Team. "Zimbabwe Forest Carbon Megaproject Generated Millions of Junk Credits." Illuminem Voices, October 1, 2025. <https://illuminem.com/illuminemvoices/zimbabwe-forest-carbon-megaproject-generated-millions-of-junk-credits>.

15 Trellis, "Volkswagen, TotalEnergies Face Risks Over 'Limbo' Carbon Credits," October 9, 2025 (updated October 13, 2025), <https://trellis.net/article/verra-kariba-investigation-risk-volkswagen-totalenergies-carbon-neutral-claims/>

16 Climate Focus, Article 6 Registry Requirements: Functional and Technical Requirements for Registries under Article 6 of the Paris Agreement (July 2014, updated October 2024), p. 4 and p. 25, <https://climatefocus.com/wp-content/uploads/2024/10/Article-6-registry-requirements-FINAL-July2014.pdf>.

17 Cambodian Carbon Registry, How It Works, accessed June 20, 2026, <https://ccr.gov.kh>.

## B. Tokenized Trading Model

In contrast, a tokenized trading converts credits into digital tokens on a blockchain through distributed ledger technology (DLT) and smart contracts<sup>18</sup>. Tokenisation may improve traceability, transparency, transactional efficiency, and accessibility. However, tokenising a carbon credit does not automatically transform it into a legally recognised digital asset or confer legal title on the token holder<sup>19</sup>. A technological record showing control over a token does not necessarily establish ownership of the underlying carbon credit unless the applicable law, registry rules, and contractual arrangements expressly connect the token to that credit<sup>20</sup>. Transferring ownership executed by smart contracts via blockchain transactions, will automatically perform contractual obligations when predetermined conditions are met and verified<sup>21</sup>.

## III. Potential Classifications of Carbon Credits

The importance of legal classification of carbon credits is to determine which authority has jurisdiction over their issuance, trading, licensing, and supervision. Under existing Cambodian law, a carbon credit could potentially be classified in one of three ways. Though each classifications contain its own strengths and weaknesses.

### 3.1. Intangible Property

According to Article 119 of CC an “Object” is defined as “a tangible object in the form of a gas, liquid or solid.”

Movables include tangible objects, but Article 120(4) of CC adds that “provisions pertaining to Movables shall apply mutatis mutandis to controllable intangible property.” Therefore, if a carbon credit is “controllable intangible property,” it could be treated analogously to a movable, allowing transfer, pledge, and enforcement under the general rules of property and contract law<sup>22</sup>. The ownership rights would be recognized and enforceable under Civil Code of Cambodia (“CCC<sup>23</sup>”).

However, this classification rises several issues. First (1) “controllable” is not defined. In the context of registry-based assets, control typically means the ability to unilaterally initiate transfers and to exclude others from doing so. The CCR could arguably provide such control. Second (2) it does not address whether carbon credits constitute as “goods” under the Law on Commercial Rules and Register (“LCRR and Its Amendment”), Under Article 1(2) of the LCRR and Its Amendment refer commercial activity as the “activity of buying or selling goods and services” that is regular and aimed at exchange and profit. Carbon credits are not clearly “goods” in the traditional sense (tangible commodities), creating interpretive uncertainty. Lastly (3) even if treated as intangible property, this classification would not bring carbon credit trading under the regulatory supervision of SERC. This means that people buying and selling them on the secondary market might be doing so without any official supervision.

Furthermore, UNIDROIT Draft Principles on the Legal Nature of Verified Carbon Credits (2025), also potentially leaning toward classifying carbon credits as intangible assets that governed by registries. While it is currently non-binding, the principle 2(1)-2(2) and 2.5 show the emerging consensus that carbon credits may be classified based on its market mechanism and transfer rules<sup>24</sup>.

18 YOUNGO (Youth Constituency of the UNFCCC), Submission by YOUNGO on the Operationalization of the Article 6.4 Mechanism, UNFCCC SBM015 (2023), section 7.2.1, [https://unfccc.int/sites/default/files/resource/SBM015\\_Call\\_for\\_input\\_annotations\\_SCP\\_Youth\\_Constituency.pdf](https://unfccc.int/sites/default/files/resource/SBM015_Call_for_input_annotations_SCP_Youth_Constituency.pdf)

19 Hassans, “Tokenised Carbon Credits: Opportunities and Key Market Distinctions,” Gibraltar Law, December 3, 2025, accessed July 7, 2026, <https://www.gibraltarlaw.com/insights/post/102lwoz/tokenised-carbon-credits-opportunities-and-key-market-distinctions/>

20 Osler, Hoskin & Harcourt LLP, “Tokenized Carbon Credits: How Blockchain Is Revolutionizing Carbon Markets,” Osler Updates, February 5, 2025, <https://www.osler.com/en/insights/updates/tokenized-carbon-credits-blockchain-revolutionizing-markets/>.

21 IBM. “What Are Smart Contracts on Blockchain?” IBM Think. <https://www.ibm.com/think/topics/smart-contracts>

22 Articles 816-842 of Civil Code of Cambodia

23 Articles 138-139 of Civil Code of Cambodia

24 UNIDROIT, Draft Principles on the Legal Nature of Verified Carbon Credits, UNIDROIT 2025 – Study LXXXVI – W.G.5, Doc. 2 rev. 13 (Rome: International Institute for the Unification of Private Law, 2025), Draft document. <https://www.unidroit.org/wp-content/uploads/2025/04/Study-LXXXVI-W.G.5-Doc.-2-rev.-Draft-Principles.pdf>

### 3.2. Securities or Derivative Instruments

One of the issues regarding tokenized carbon credits in Cambodia is whether under the Law on the Issuance and Trading of Non-Government Securities (“**LITINGS**”), should it be classified as (a) securities or (b) derivative instrument. This classification is needed, as it will be determining regulatory jurisdiction over the issuance and trading of tokenized carbon credits.

(a) Under the Article 7 of the LITINGS, which gives SERC authority to govern and oversee the investment that are related to financial activities which includes financial technologies and digital asset markets. In addition, LITINGS’s annex glossary define the non-government securities as“(a) ownership securities such as shares, (b) debt securities such as bonds, (c) Interest in a Managed Investment Scheme; (d) future instrument or derivative instrument related to securities based on (a) (b) and (c); and (e) other financial instrument determined as securities<sup>25</sup>.” Moreover, SERC’s Guideline on FinTech Regulatory Sandbox in the Securities Sector also demonstrate that tokenized assets that fall under the definition of “securities” may be subject to SERC’s licensing and supervisory powers<sup>26</sup>.

(b) If carbon credits are classified as derivative instruments, trading platforms would need to obtain these licenses and comply with the regulations in accordance with on the Prakas No. 005/20 SERC/PK Amendment on the Prakas No. 004/15 SERC/PK on Licensing and Management of Derivative Instrument Trading (“**Prakas 005/20 SERC/PK**”). Pursue to Article 15 (New) of Prakas No. 005/20 SERC/PK states that Central Counterparty (CCP), derivative brokers, derivative representative must obtain licenses from SERC and comply with capital requirements.

On 05 February 2024, KS Green Co., Ltd., South Korean company, had signed a Memorandum of Understanding (“MOU”) with SERC to applied the FinTech Regulatory Sandbox to launch Cambodia’s first Security Token Offering (“STO”) exchanges specializing in carbon credits<sup>27</sup>. Afterward, on 14 April 2025, KS Green officially graduated from sandbox and became the first to received license to operate an STO exchange based on various real assets in Cambodia<sup>28</sup>. Even though the license does not explicitly for tokenized carbon credits, it nevertheless shows Cambodia’s openness toward blockchain-based and tokenized assets market.

On 26 December 2024, NBC issued Prakas on Transactions Related to Cryptoassets (“Prakas on Cryptoasset”) aim to control the flow of transaction and manage the business activities in relation to cryptoassets. Under Article 3 of Prakas on Cryptoasset, which defines tokenization as a legal and technological process competent of attaching enforceable rights to blockchain-based digital systems. This shown that Cambodian regulators acknowledged the rights between blockchain entries and its legal effect.

Needless to say, carbon credit itself is not a share, bond, or managed investment scheme interest. Even the catch-all “other financial instrument determined as securities” scope gives SERC discretion, but it has not yet been exercised for carbon credits<sup>29</sup>. It only shows that KS Green’s STO successful licensing shows that SERC is willing to grant licenses for tokenized asset platforms under its existing authority.

### 3.3. Sui Generis

A third path is to acknowledge that carbon credits fit none of the existing categories and therefore require a sui generis legal regime. ENR Code establishes principles of environmental protection and sustainable resource management that could support recognizing carbon credits as a form of environmental asset and climate change response measures<sup>30</sup>. Under Article 9 of the ENR Code, the principle of sustainable development requires that “All economic and social development activities shall fulfill the developmental and environmental needs of people and future generations in an equitable and sustainable manner...”. Moreover, Article 13 of ENR Code provides that “All persons who cause harm to the environment shall bear the cost of repairing the damage.”. But these do not create a property framework for carbon credits.

A *Sui Generis* solution would mean enacting new legislation that defines carbon credits as a distinct asset class, specifies the rights and obligations of holders, designates a regulatory authority (or dual authorities), and provides for registration, transfer, and enforcement. However, this model emerges as the superior line

25 Annex Glossary of Law on the Issuance and Trading of Non-Government Securities, p.3

26 Guideline on Fintech Regulatory Sandbox in the Securities Sector No. 009/23 SERC/K.N.N

27 KhmerTimes “Cambodia’s Emerging 1st STO Exchange; Specialized in Carbon Credit.” February 8, 2024. <https://www.khmertimeskh.com/501436858/cambodias-emerging-1st-sto-exchange-specialized-in-carbon-credit/>.

28 Jung Jin, “KS GREEN Receives Cambodia’s First STO Exchange License. Building Asia Europe Digital Finance Hub,” Asia Business Daily, April 14, 2025, accessed June 20, 2026, <https://www.asiae.co.kr/en/article/2025041413572848146>.

29 Annex Glossary of Law on the Issuance and Trading of Non-Government Securities, p.3

30 Articles 64-85 of Environmental and Natural Resources Code



of reasoning for Cambodia's long-term development. Despite having its own flaw in require a great demand legislative investment upfront, by having a dedicated law governing carbon credits can simultaneously (i) classify the carbon credits, (ii) competent authorities oversee, (iii) establish proper licensing for platforms, (iv) enable pledge by control, and (v) provide for third-part enforceability.

## IV. Comparative Approaches in Indonesia and Malaysia

This comparative shows that carbon classification issue is not unique issue for Cambodia, as other ASEAN members also face similar challenges when it comes to alignment with carbon market models and their economic. By illustrate the example of how each model operates in practice, to reduce the risk and cost of legislative experimentation for Cambodia. Indonesia was selected because they classified their carbon unit as securities instrument, while Malaysia was chosen for their VCM. Despite Indonesia, and Malaysia are classified as upper-middle-income economies<sup>31</sup>, and Cambodia is still classified as a lower-middle-income economies, by sharing the ASEAN membership and regional integration framework making Indonesia and Malaysia are more persuasive than distant jurisdictions.

### 4.1. Indonesia

Carbon units as classified as securities (efek) under Article 3(1) of the OJK Regulation No. 14/2023 (POJK 14/2023). These transform the carbon units into a tradeable assets and alleageable financial collateral under the OJK-supervised. Since it fell under securities instrument, there is a need for licensing in order to trade carbon through Carbon Exchange<sup>32</sup>. Indonesia operates under the cap-and-trade compliance systems for emission allowance and offsets in according with the Presidential Regulation No. 110/2025<sup>33</sup>. Meanwhile, pursue to Article 68 of MOEF Regulation No. 21/2022, trading carbon generated by Indonesian projects inter-nationally requires MOEF's authorization to avoid double counting and ensure market integrity.

Cambodia should also impose clear definition of carbon credits as intangible assets, with verifier accreditation framework and a clear division between voluntary credits and ITMOs.

### 4.2. Malaysia

In contrast, Malaysia does not have a legislation that specifically govern carbon credits as a tradable instrument rather the transactions were governed by general contract law<sup>34</sup>. In December 2022, Bursa Carbon Exchange ("BCX") was launched as the first Shariah-Compliant VCM platform<sup>35</sup>. BCX set out the rules and procedures regarding processes and requirement that participants must comply to<sup>36</sup>. In VCM model, there is no restriction imposed on the sales of carbon generated from projects located in Malaysia to buyers outside the country<sup>37</sup>.

Pursuing to Section 70A of the Sarawak Forests Ordinance (2015) encourages Director of Forests to grant a "Forest Carbon License" for forest carbon activities in any permanent forest, state land, or alienated land. Furthermore, in subsection 70A(2) grants legal and beneficial title to carbon or GHG stock that co-related with forest carbon activity. In July 2025, Sabah passed the Climate Change and Carbon Governance, establishes Sabah Climate Action Council as high-level decision-making body<sup>38</sup>.

31 World Bank Group. n.d.a. Malaysia – Economy Overview. Accessed June 20, 2026. <https://www.worldbank.org/ext/en/country/malaysia#tab-economy>.; World Bank Group. n.d.b. Indonesia – Economy Overview. <https://www.worldbank.org/ext/en/country/indonesia#tab-economy>.

32 Rudi Bachtiar and Salsabila Safira, "New Carbon Exchange Regulation — ESG and Climate Change Update," ARMA Law, November 2023, <https://www.arma-law.com/news-event/newsflash/esg-and-climate-change-carbon-exchange-regulation>.

33 Republic of Indonesia, Presidential Regulation Number 110 of 2025 concerning the Implementation of Carbon Economic Value Instruments and National Greenhouse Gas Emission Control, October 10, 2025, InforMEA, <https://www.informea.org/en/content/legislation/presidential-regulation-number-110-2025-concerning-implementation-carbon>.

34 Bird & Bird, Carbon Credits Framework Comparison across Singapore, Malaysia & Indonesia, in collaboration with Nurjadin Sumono Mulyadi & Partners and Azmi & Associates, May 17, 2024, p. 4.

35 Bursa Malaysia Carbon Exchange. n.d. An Investor's Guide to Voluntary Carbon Markets. [https://bcx.bursamalaysia.com/insightsevents\\_subpage/an-investors-guide-to-voluntary-carbon-markets-nav-13.html](https://bcx.bursamalaysia.com/insightsevents_subpage/an-investors-guide-to-voluntary-carbon-markets-nav-13.html).

36 Bursa Malaysia Carbon Exchange, Rules of Bursa Carbon Exchange, May 6, 2024, ch. 1, secs. 1.03–1.06.

37 Bursa Malaysia Carbon Exchange, Voluntary Carbon Market Handbook, v1.2.1, 2024, 12.

38 Ravinyaa Ravimalar, "Sabah: Capitalising on the Country's Net Carbon Sink," The Edge Malaysia, January 1, 2026, <https://theedgemaalaysia.com/node/787546>.

By adopting similar operational flexibility, Cambodia should consider providing licensing to confer legal title to project proponents, which allow rules to adapt without frequent amendment, while building bilateral agreements with the Article 6 of Paris Agreement.

## **V. The Necessity of Dedicated Carbon Credit Legislation**

### **5.1. Cambodia's Existing Legal Framework Cannot Classify Carbon Credits**

The analysis in Section III shows that neither the intangible property nor the securities or derivative instrument classification fits cleanly. On one hand the CC's tangible-object requirement blocks full property treatment. On the other hand, the securities laws do not clearly include them as derivatives. And the ENR Code provides principles but no operational rules for ownership, transfer, or enforcement. CCR can record who controls an account; it can issue serial numbers and track transfers. But unless the underlying law recognizes that control as property, the registry entry is merely evidence of an administrative fact, not a legal title.

### **5.2. A Framework for Legislative Reform**

The following recommendations are based on the concrete legal consequences found in the gaps identified above. First, carbon credits should be defined as regulated intangible assets. By not having intervention from the government, a court may treat carbon trading as a mere contractual right with an inadequate third-party effect. As a result, a creditor cannot seize a credit and a bank cannot accept it as collateral. Therefore, giving carbon credit a proprietary title, unlocking the commercial potential of Cambodia's carbon assets.

Second, oversight must be split between MOE and SERC when it comes to trading carbon on the platform. Carbon credits by themselves are an environmental instrument, by trading on a digital marketplace, merge both environmental and financial characteristics together. MOE holds expertise in project validation, verification, credit issuance, retirement, and corresponding adjustments under Article 6 of Operation Manual. While, SERC holds competence in licensing trading platforms, and supervising digital markets. By splitting responsibilities based on the expertise of the ministries can ensure both environmental and market integrity are both regulated.

## **VI. Conclusion**

The question is no longer whether Cambodia should legislate, but when and how well. The path to a functional, high-integrity carbon market begins with a clear legal definition of the credit itself. Existing Cambodian law cannot resolve these gaps until the legal nature of carbon credits is clearly defined. Through an analysis of Cambodian property, securities, environmental, and digital-asset regulation, it concludes that carbon credits are most appropriately recognized as intangible assets that subject to a specialized regulatory framework.

Nevertheless, legal classification alone will not resolve every difficulty. The effectiveness of the market will also depend on environmental integrity, registry reliability, clear rules on transfer and third-party rights, and coordination between regulatory authorities. The Ministry of Environment should supervise the environmental validity and issuance of carbon credits, while the Securities and Exchange Regulator of Cambodia should oversee market conduct where credits are traded as investment or tokenised instruments. Any regulation of tokenised credits must also remain consistent with the National Bank of Cambodia's rules concerning cryptoassets.

This study is limited to the legal classification and regulatory treatment of carbon credits under the existing Cambodian framework. It does not examine in detail taxation, accounting treatment, insolvency, consumer protection, or the distribution of benefits among project developers, landholders, and local communities. These issues may affect how the proposed classification operates in practice.

Future research should therefore examine the treatment of carbon credits in secured transactions and insolvency, the legal effect of entries in the Cambodia Carbon Registry, and the protection of community and land-related rights in carbon projects. Such research would complement the present findings and assist Cambodia in developing a coherent, credible, and high-integrity carbon market.

## Bibliography

### Law and Regulations

1. Civil Code of Cambodia,
2. Environmental and Natural Resources Code of Cambodia.
3. Law on the Issuance and Trading of Non-Government Securities.
4. Prakas No. 005/20 Amendment on the Prakas No. 004/15 SERC/PK on Licensing and Management of Derivative Instrument Trading.
5. Prakas on Transaction Related to Cryptoassets.
6. Office of Council of Ministers. Letter No. 1380 Sor Chor Nor. Dor Bor.
7. Otoritas Jasa Keuangan [Financial Services Authority]. Regulation Number 14 of 2023 concerning Carbon Trading through Carbon Exchanges.
8. Republic of Indonesia. Presidential Regulation Number 110 of 2025 concerning the Implementation of Carbon Economic Value Instruments and National Greenhouse Gas Emission Control.
9. Operations Manual for the Implementation of Article 6 of the Paris Agreement on Climate Change in Cambodia.

### Reports/ Institutional Publications

1. Bird & Bird. Carbon Credits Framework Comparison across Singapore, Malaysia & Indonesia. In collaboration with Nurjadin Sumono Mulyadi & Partners and Azmi & Associates. <https://www.twobirds.com/-/media/new-website-content/insights/pdfs/joint-publication-bb-nsmp-aa-carbon-credits-comparison-across-singapore-malaysia-indonesia-17-may.pdf>
2. Bursa Malaysia Carbon Exchange. Rules of Bursa Carbon Exchange. [https://bcx.bursamalaysia.com/pdf/resources/rules\\_bursacarbon.pdf](https://bcx.bursamalaysia.com/pdf/resources/rules_bursacarbon.pdf)
3. Bursa Malaysia Carbon Exchange. Voluntary Carbon Market Handbook. v1.2.1. [https://www.bursa-malaysia.com/sites/5d809dcf39fba22790cad230/assets/685cfcc9cd34aaa86530631d/VCM\\_Handbook\\_Final\\_V1.2.1.pdf](https://www.bursa-malaysia.com/sites/5d809dcf39fba22790cad230/assets/685cfcc9cd34aaa86530631d/VCM_Handbook_Final_V1.2.1.pdf)
4. Cambodian Carbon Registry. How It Works. Ministry of Environment, Kingdom of Cambodia. <https://ccr.gov.kh/how-it-works>
5. Climate Focus. Article 6 Registry Requirements: Functional and Technical Requirements for Registries under Article 6 of the Paris Agreement. [https://climatefocus.com/wp-content/uploads/2024/10/Article-6-registry-requirements-FINAL\\_July2014.pdf](https://climatefocus.com/wp-content/uploads/2024/10/Article-6-registry-requirements-FINAL_July2014.pdf)
6. European Commission. EU ETS Handbook. Brussels: Directorate-General for Climate Action [https://climate.ec.europa.eu/system/files/2017-03/ets\\_handbook\\_en.pdf](https://climate.ec.europa.eu/system/files/2017-03/ets_handbook_en.pdf).
7. UNIDROIT. Draft Principles on the Legal Nature of Verified Carbon Credits. UNIDROIT 2025 – Study LXXXVI – W.G.5, Doc. 2 rev. 13. Rome: International Institute for the Unification of Private Law, 2025. <https://www.unidroit.org/wp-content/uploads/2025/05/Study-LXXXVI-W.G.5-Doc.-3-Summary-Report.pdf>
8. United Nations Development Programme. What Are Carbon Markets and How Do They Work? Climate Promise. <https://climatepromise.undp.org/news-and-stories/what-are-carbon-markets-and-how-do-they-work>
9. World Bank Group. Malaysia – Economy Overview. <https://www.worldbank.org/ext/en/country/malaysia>
10. World Bank Group. Indonesia – Economy Overview. <https://www.worldbank.org/ext/en/country/indonesia>
11. YOUNGO (Youth Constituency of the UNFCCC). Submission on the Operationalization of the Article 6.4 Mechanism. [https://unfccc.int/sites/default/files/resource/SBM015\\_Call\\_for\\_input\\_annotations\\_SCP\\_Youth\\_Constituency.pdf](https://unfccc.int/sites/default/files/resource/SBM015_Call_for_input_annotations_SCP_Youth_Constituency.pdf).

### Journal/News Articles

1. Fan, Jing-Li, et al. "Global Carbon Market: A Review of the Current Status, Challenges, and Future Prospects." Environmental Science and Ecotechnology 21 <https://doi.org/10.1016/j.es.2024.100412>.
2. ARMA Law. "New Carbon Exchange Regulation — ESG and Climate Change Update." November 2023. <https://www.arma-law.com/news-event/newsflash/esg-and-climate-change-carbon-exchange-regulation>
3. Illuminem Editorial Team. "Zimbabwe Forest Carbon Megaproject Generated Millions of Junk Credits." Illuminem Voices. <https://illuminem.com/illuminemvoices/zimbabwe-forest-carbon-megaproject-generated-millions-of-junk-credits>
4. Jin, Jung. "KS GREEN Receives Cambodia's First STO Exchange License... Building Asia Europe Digital Finance

Hub." Asia Business Daily.

5. Khmer Times. "Cambodia's Emerging 1st STO Exchange; Specialized in Carbon Credit." <https://www.khmer-timeskh.com/501436858/cambodias-emerging-1st-sto-exchange-specialized-in-carbon-credit/>
6. Khmer Times. "Environment Ministry Launches Carbon Registry for Transparency, Accountability." [https://www.khmertimeskh.com/501782990/environment-ministry-launches-carbon-registry-for-transparency-accountability/#google\\_vignette](https://www.khmertimeskh.com/501782990/environment-ministry-launches-carbon-registry-for-transparency-accountability/#google_vignette)
7. Ravinyaa Ravimalar. "Sabah: Capitalising on the Country's Net Carbon Sink." The Edge Malaysia. <https://theedgemalaysia.com/node/787546>.
8. Trellis. "Volkswagen, TotalEnergies Face Risks Over 'Limbo' Carbon Credits." <https://trellis.net/article/vera-kariba-investigation-risk-volkswagen-totalenergies-carbon-neutral-claims/>
9. Osler, Hoskin & Harcourt LLP. "Tokenized Carbon Credits: How Blockchain Is Revolutionizing Carbon Markets." Osler Updates, February 5, 2025. <https://www.osler.com/en/insights/updates/tokenized-carbon-credits-blockchain-revolutionizing-markets/>.
10. EcoVadis Editorial Team. "Carbon Tax: Understanding Supply Chain Cost Exposure." EcoVadis Blog, June 23, 2026. <https://ecovadis.com/blog/carbon-tax/>.



## **Licensing Foreign Cryptoasset Service Providers in Cambodia:**

### **A Legal Analysis of Registration Barriers**

*TAING Kimsuo*



## Abstract

Cambodia's emerging regulatory framework for cryptoasset service providers ("**CASP**") seeks to strengthen consumer protection, anti-money laundering compliance, and regulatory oversight. However, several licensing requirements introduced under the Prakas on the Issuance of License and Management of Digital Asset Business create significant barriers for established foreign crypto exchanges seeking to operate legally in Cambodia. This law brief examines three principal obstacles: the residency requirement for key personnel, the obligation to maintain a local data center, and the mandatory completion of a domestic regulatory sandbox. Through comparative analysis of regulatory approaches adopted in other jurisdictions, the brief argues that these requirements are disproportionate when applied to globally regulated platforms. It proposes a more flexible, equivalence-based framework, including the adoption of a local compliance officer model, recognition of foreign cybersecurity and data governance standards, and a tiered market entry system. Such reforms would enable Cambodia to bring reputable international exchanges within its supervisory framework, thereby increasing oversight to protect Cambodian users, while preserving the borderless nature of digital finance and maintaining robust AML/CFT safeguards.

## I. Introduction

Cambodia continues to rank highly in crypto adoption, breaking into the top 13 of the 2025 Global Crypto Adoption Index compared to Singapore, which ranks 15th<sup>1</sup>. In November 2024, Cambodia blocked 16 unlicensed crypto exchange websites, including Binance and Coinbase, through directives that cited consumer protection and anti-money laundering concerns<sup>2</sup>. Yet, Cambodian users were still able to use such platforms using Virtual Private Networks (VPNs) or mobile applications, and the transactions that motivated the ban continued uninterrupted<sup>3</sup>. The outcome inadvertently created a gray legal zone, limiting the ability of Cambodian authorities to supervise these platforms while driving consumers away from regulated global exchanges and into less transparent channels. The ban has thereby inadvertently pushed consumers into illegality without providing any pathway to regularization.

On December 2024, the National Bank of Cambodia ("**NBC**") adopted the Prakas on the Transaction Related to Cryptoassets ("**NBC Prakas**"), which mandated the licensing of Cryptoasset Service Providers ("**CASP**") but delegated the actual licensing mechanism to a subsequent Prakas that is currently being drafted<sup>4</sup>. A year later, in December 2025, the Securities and Exchange Regulator of Cambodia ("**SERC**") issued the Prakas on the Issuance of License and Management of Digital Asset Business ("**SERC Prakas**"). The two Prakas use different terms to address each service provider, whereas the NBC Prakas uses CASPs and SERC Prakas uses Digital Asset Service Provider ("**DASP**"). However, both CASPs and DASPs provide overlapping service including the exchange of cryptoassets against official currencies or other assets, transfer services, and the safekeeping, custody, or administration of digital assets on behalf of customers<sup>5</sup>. The SERC Prakas itself acknowledges this overlap, requiring joint guidelines to reconcile between the two regulatory authorities over digital asset operations<sup>6</sup>. For the purposes of this law brief, the term CASPs is used throughout.

A few conditions in the SERC Prakas, such as local residency requirements for key personnel<sup>7</sup>, local data center<sup>8</sup>, and completion of a domestic regulatory sandbox<sup>9</sup>, make it practically difficult for established foreign crypto exchanges to obtain a license in Cambodia. This is because such platforms operate cryptoassets that are inherently global in nature, assets that cannot be meaningfully localized without undermining the core value proposition they offer<sup>10</sup>. This creates a significant tension. On one hand, Cambodia has legitimate reasons for these requirements: strengthening regulatory oversight, promoting the use of the local currency,

1 Chainalysis Team, "The 2025 Global Adoption Index: India and the United States Lead Cryptocurrency Adoption," Chainalysis, September 2, 2025, <https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/>.

2 Tareq Sikder, "Coinbase, Binance Among 16 Crypto Exchange Websites Blocked by Cambodia," Finance Magnates, December 04, 2024, <https://www.financemagnates.com/cryptocurrency/coinbase-binance-among-16-crypto-exchange-websites-blocked-by-cambodia/>.

3 Brandon Tan Jun Wen, "The Flawed Approach of Cambodia's Cryptocurrency Ban," Fulcrum Analysis of Southeast Asia, January 9, 2025, <https://fulcrum.sg/the-flawed-approach-of-cambodias-cryptocurrency-ban/>.

4 Art. 3 of NBC Prakas; Cambodia's 2nd National Risk Assessment Report on Money Laundering and Terrorist Financing (NRA II), (2025), p.13.

5 Art. 20 of NBC Prakas; Art. 4 of SERC Prakas.

6 Art. 60 of SERC Prakas.

7 Art. 8 of SERC Prakas.

8 Art. 15(13) of SERC Prakas,

9 Art. 8(3) of SERC Prakas, FinTech Regulatory Sandbox refer to an environment for FinTech institutions to experiment their services and products with real customers, but within a certain size and time before launching and promoting widespread use. Digital Economy and Business Committee, *Cambodia Financial Technology Development Policy 2023-2028*, (Cambodia: 2023), Annex 2. Glossary, p.39.

10 Robby Houben, Alexander Snyers, *Crypto-assets: Key developments, regulatory concerns and responses*, (Luxembourg: European Parliament, 2020), p.10.

and distancing itself from its reputation as a haven for cybercriminals and scam operations<sup>11</sup>. On the other hand, excluding reputable foreign exchanges leaves Cambodian investors with limited safe options and risks using platforms that operate without Cambodia oversight.

Acknowledging this tension is not a concession that the regulatory goals are wrong, but a recognition that the chosen means of achieving them may be disproportionate in particular in the absence of any proposed path towards regularization for existing crypto asset holders and users in the implementation phase. Moreover, the National Risk Assessment II found that Cambodia's Virtual Asset sector presents a medium-high level of risk, with residual risks largely arising from activities conducted through foreign exchanges<sup>12</sup>. Therefore, this brief does not seek to advocate for an unrestricted influx of foreign companies into Cambodia, but rather examines the conditions under which foreign crypto platforms could obtain a Cambodian license, thereby bringing them within the supervisory authority of Cambodian regulators, especially for Anti-Money Laundering /Combating the Financing of Terrorism ("AML/CFT") purposes. Such an approach is also consistent with the Financial Action Task Force ("FATF") recommendation that jurisdictions may require Virtual Asset Service Providers offering products and services to customers within their territory to be licensed<sup>13</sup>.

The previous law brief has examined how cryptocurrency frameworks operate globally, typically emphasizing strict local licensing, regulatory sandboxes, and structural oversight to mitigate financial risks and prevent money laundering<sup>14</sup>. However, there is a lack of research on the regulation of foreign crypto exchange platforms. Further analysis is required to address the cross-border nature of cryptoassets, which differ fundamentally from traditional financial systems, and the fact that cryptoassets cannot circulate effectively without exchange platforms.

The legal problem examined in this brief concerns the legal consequences stemming from the exclusion of established foreign crypto exchanges from local licensing as produced by the SERC Prakas. At the heart of this problem, there are 3 sub-problems, which this brief proposes to analyze. In section 1, examines the residency requirement for key personnel and proposes a more flexible approach to ensuring regulatory accountability. Section 2 analyzes the local data center requirement and proposes an equivalence-recognition mechanism. Lastly, section 3 assesses the mandatory domestic sandbox requirement and proposes an equivalence-based approach.

## **II. Reconciling Physical Presence Mandates with the Borderless Architecture of Digital Finance**

### **1.1. The Residency Requirement and the Structure of Global Cryptoasset Platforms**

A licensing condition imposed on CASPs under the SERC Prakas requires that the Director, Chief Executive Officer, and other key personnel of a licensed entity maintain residency in the Kingdom of Cambodia<sup>15</sup>. The purpose of this requirement is presumably to ensure that senior decision-makers are personally accountable to Cambodian regulatory authorities and that the management of a licensed entity is not conducted entirely from abroad, beyond the reach of enforcement action. For a domestically incorporated start-up or a locally focused financial institution, this requirement presents no particular difficulty. For a globally integrated platform operating under a centralized compliance model, however, the requirement is structurally incompatible with the entity's organizational structure.

A threshold interpretive difficulty is that the SERC Prakas does not define the term 'residency'. However, under the Cambodian Civil Code (CCC) residence is typically associated with domicile which is a person's base and center of living<sup>16</sup>. Applied strictly, this would indeed require relocation of the relevant executives to Cambodia. An alternative and more workable interpretation would construe 'residency' as denoting 'effective presence', defined functionally as the demonstrated capacity to respond to regulatory enquiries within a defined timeframe, attend required supervisory meetings either in person or by remote means, and exercise meaningful decision-making authority over the Cambodian operations of the platform. Under this reading, the residency condition becomes a standard of operational responsiveness and supervisory accountability rather than a mandate for physical residency.

11 Brandon Tan Jun Wen, "The Flawed Approach of Cambodia's Cryptocurrency Ban," op. cit.

12 Cambodia's 2nd National Risk Assessment Report on Money Laundering and Terrorist Financing (NRA II), op. cit, p.13.

13 FATF, *International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation: The FATF Recommendations*, (Paris: 2025), p.78.

14 KAS, *Law Brief 2.0: Digital Law*, (Cambodia: 2024), p.34.

15 Art.10(2) of SERC Prakas,

16 Art. 34 of Civil Code, No. NS/RKM/1207/030, 08 December 20,,.

This functional reading is supported by comparative practice. The Bank for International Settlements has noted that the purpose of senior management localization requirements is to ensure supervisory access and accountability, not physical co-location<sup>17</sup>. A functional interpretation of the term ‘residency’ that achieves the same regulatory objectives through accountability mechanisms rather than through a relocation requirement may therefore provide a more proportionate solution.

## 1.2. Compliance Officer Model as a Proportionate Alternative

The European Union’s Markets in Crypto-Assets Regulation (“**MiCA**”) requires that, to ensure effective supervision and prevent the evasion of rules, CASPs must have at least one director who is a resident in the Union<sup>18</sup>. Similarly, in Singapore, the Payment Services Act requires that at least one director of a licensee be a Singapore citizen or permanent resident<sup>19</sup>. Furthermore, every licensee must appoint at least one natural person to be physically present at its registered place of business for the purpose of addressing customer queries and regulatory correspondence<sup>20</sup>.

Cambodia could adopt a comparable model, tailored to its own regulatory context. Accordingly, the appropriate reform would be to amend the Prakas to require, first, that at least one Director be a Cambodian citizen or permanent resident and, second, that every licensed CASP appoint a dedicated Regulatory Compliance Officer (“**RCO**”) to reside in Cambodia. The RCO would be required to: (i) be a natural person resident in Cambodia; (ii) hold personal regulatory accountability for the CASPs AML/CFT compliance in Cambodia; (iii) have direct authority to respond to SERC supervisory requests; and (iv) be subject to personal sanctions for compliance failures. This model separates the regulatory accountability function, which must be local, from the governance function, which can remain global. It is proportionate, legally coherent, and consistent with international best practice.

Therefore, in the immediate term, SERC can issue interpretive guidance confirming that the existing residency condition may be satisfied by ‘effective presence’ as defined functionally, thereby removing a structural barrier to licensing without requiring legislative amendment. This would provide immediate regulatory certainty and signal Cambodia’s openness to well-governed international platforms. Alternatively, SERC can pursue a formal amendment to the Prakas to include the RCO model, establishing clear statutory obligations, defined liability standards, and an enforceable supervisory relationship between SERC and a locally present compliance officer for each licensed CASP.

## III. Bridging Local Data Center Requirement with Equivalence-Recognition Framework

One of the requirements for CASP licensing is that the applicant must be a ‘company registered for commerce in the Kingdom of Cambodia’<sup>21</sup>. A foreign company can register with the Ministry of Commerce in Cambodia (MOC) if they are doing business locally in the form of a representative office, branch, or subsidiary<sup>22</sup>. The Law on Commercial Enterprises (LCE) stipulates that ‘doing business’ means that the company rents or occupies space to provide services or employs personnel for at least one month<sup>23</sup>.

However, an additional condition under the SERC Prakas requires CASPs to maintain a physical data center presence within Cambodia<sup>24</sup>. Presumably, this condition is imposed to ensure regulatory oversight, data sovereignty, and investor protection. Consequently, this requirement creates significant barriers for foreign companies, as establishing a local data center is costly and technically demanding, especially for firms that already operate secure, compliant infrastructure abroad.

Other jurisdictions have adopted more flexible approaches. In the European Union under MiCA, foreign CASPs can operate across member states once licensed, without mandatory local data centers, though they must comply with strict cybersecurity and governance standards<sup>25</sup>. Under Singapore’s Monetary Authority of Singapore framework, a digital payment token service provider (the Singaporean equivalent of a CASP) is required to maintain a permanent place of business or registered office in Singapore where its books of transactions must be kept; however, the Act does not explicitly mandate a local data center<sup>26</sup>.

17 Basel Committee on Banking Supervision, Core Principles for effective banking supervision, (2024), p.21.

18 Regulation (EU) 2023/1114 on Markets in Crypto-assets, 31 May 2023, Article 59(2).

19 Singapore Payment Service Act, 31 December 2021, Section 6(9).

20 Singapore Payment Service Act, 31 December 2021, Section 14(2).

21 Art. 4 of SERC Prakas.

22 Law on Commercial Enterprises of Cambodia, No. NS/RKM/060/019, 19 June 2005, Article 271 New.

23 Law on Commercial Enterprises of Cambodia, No. NS/RKM/060/019, 19 June 2005, Article 272 New.

24 Art. 15(13) of SERC Prakas

25 Regulation (EU) 2023/1114 on Markets in Crypto-assets, 31 May 2023, Article 68(7); Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, 14 December 2022, para.82. Digital Operational Resilience for the Financial Sector, 14 December 2022, para.82.

26 Singapore Payment Service Act, 31 December 2021, Section 6.

As of 2026, Singapore had licensed foreign platforms such as Coinbase and OKX<sup>27</sup>. Dubai's Virtual Assets Regulatory Authority ("VARA") regulations do not explicitly require a local data center; however, they ensure robust data systems by mandating that VASPs implement a comprehensive Technology Governance and Risk Assessment Framework, conduct annual independent security audits, and provide the authority with access to information regardless of its storage location<sup>28</sup>. Notably, Dubai has licensed major global exchanges such as Binance, Crypto.com and OKX<sup>29</sup>.

However, for Cambodia, simply eliminating this requirement would create a new vulnerability, as it could allow companies with weak information and cybersecurity systems to bypass oversight entirely. Therefore, a better approach would be to introduce a disjunctive condition that allows an applicant to either establish a local data center or provide proof of a robust information and cybersecurity system. This proof could be demonstrated through methods such as audits, certifications, and cooperation with SERC inspections. Alternatively, Cambodia could adopt a robust framework similar to Dubai's VARA, which grants the SERC or supervisory authorities' access to data regardless of its physical storage location, thereby demonstrating that their system has sufficient capacity, stability, and security for business operations in Cambodia<sup>30</sup>. This approach preserves Cambodia's regulatory objectives while lowering entry barriers for reputable foreign companies. It also aligns Cambodia with international best practices, encouraging innovation and foreign investment while maintaining strong oversight.

#### **IV. The Disproportionality of Universal Sandbox Testing for Already-Regulated Global Platforms**

Another requirement for a CASP license is that market entry is conditional upon the successful completion of a domestic financial technology sandbox<sup>31</sup>. The sandbox mechanism, originally developed by the UK Financial Conduct Authority as a tool for testing novel fintech products in a controlled regulatory environment<sup>32</sup>, serves a legitimate purpose when applied to genuinely new, untested products. It allows regulators to assess systemic risks, consumer protection implications, and technical reliability before granting full market authorization.

However, global platforms such as Binance, which processes hundreds of billions of dollars in transactions annually and operates under regulatory oversight in multiple major jurisdictions. Consequently, this requirement would be unnecessary and an obstacle for such platforms because the informational purpose of the sandbox (collecting data on how a product behaves) cannot be served by testing a product whose behavior is already comprehensively documented by years of live operation under regulated conditions. Therefore, applying sandbox requirements uniformly to novel products and established platforms alike conflates two categorically distinct regulatory problems.

The principle of proportionality in regulatory law requires that a regulatory measure be suitable, necessary, and proportionate in the strict sense to the legitimate aim pursued<sup>33</sup>. A sandbox requirement that produces no additional regulatory information, because the information already exists in the form of foreign supervisory records, audit reports, and compliance documentation, is therefore not necessary in the required sense. An equally effective alternative, producing lower costs for regulated entities, is available, which is the assessment of foreign regulatory equivalence.

The amendment of this requirement to introduce a tiered market entry model can be a solution to this problem. Tier 1 would apply to novel domestic products with no prior regulatory history, for which the full sandbox process remains appropriate. Tier 2 would apply to established foreign platforms regulated in FATF-compliant jurisdictions, for which sandbox requirements are replaced by an equivalence certification process. The applicant submits its home-jurisdiction regulatory authorization, audit history, and AML/CFT compliance documentation<sup>34</sup>. The SERC would assess whether the home regime meets a defined equivalence standard, and upon certification, the platform would receive a provisional market authorization subject to ongoing supervisory reporting<sup>35</sup>.

27 "Coinbase Singapore Pte. Ltd." Monetary Authority of Singapore, <https://eservices.mas.gov.sg/fid/institution/detail/235467-COINBASE-SINGAPORE-PTE-LTD> & "OKX SG Pte. Ltd.", Monetary Authority of Singapore, <https://eservices.mas.gov.sg/fid/institution/detail/422854-OKX-SG-PTE-LTD>

28 Dubai Virtual Assets Regulatory Authority, Technology and Information Rulebook, (Dubai: 2025), p.5, 10 & 17.

29 Lockridge Okoth, "Kraken Wins Major License in Dubai, Binance and OKX to Face New Competition", Yahoo Finance, 21 May 2026, <https://finance.yahoo.com/markets/crypto/articles/kraken-wins-major-license-dubai>

30 Art. 15 of SERC Prakas.

31 Art. 8(3) of SERC Prakas,

32 "Regulatory Sandbox", Financial Conduct Authority, March 06, 2026, <https://www.fca.org.uk/firms/innovation/regulatory-sandbox>

33 *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the, protection of personal data*, (2019), p.3.

34 Art. 8(14) of SERC Prakas,

35 Art. 8(3) of SERC Prakas,

## V. Conclusion

This brief has demonstrated that the current licensing framework for CASPs, while pursuing legitimate regulatory goals, protect Cambodian users from unlicensed crypto platforms, imposes disproportionate barriers on established foreign platforms through strict residency, local data center, and sandbox requirements. By transitioning toward a functional, equivalence-based regulatory model, specifically through the adoption of a RCO model and a tiered market entry system, Cambodia can bring global exchanges under its supervisory authority without undermining their borderless operational architecture. Such approach ensures that regulatory accountability is localized while allowing Cambodia to benefit from the security and liquidity of reputable international platforms.

It is important to acknowledge the limitations of this study. Due to the specific focus on the immediate licensing hurdles created by the SERC Prakas, this analysis did not extensively address the broader legal complexities of Decentralized Finance (DeFi) or the technical nuances of cross-chain interoperability, which may present unique jurisdictional challenges. These elements were excluded to maintain a precise and well-structured legal analysis focused on the immediate barriers to entry for foreign exchanges. These limitations provide a foundation for future legal research within the Cambodian innovation economy. By addressing these adjacent issues, the Cambodian legal community can continue to refine a regulatory landscape that balances robust oversight with the demands of a globalized digital economy.



## Bibliography

### Laws and Regulatory Instruments

#### Cambodia

1. Civil Code of the Kingdom of Cambodia (2007).
2. Law on Commercial Enterprises of the Kingdom of Cambodia (2005).
3. Prakas on the Transaction Related to Cryptoassets (2024).
4. Prakas on the Issuance of License and Management of Digital Asset Business (2025).

#### Other Jurisdiction

1. Regulation (EU) 2023/1114 on Markets in Crypto-assets (2023)
2. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (2022)
3. Singapore Payment Service Act (2021)

#### Books

1. Cambodia's 2nd National Risk Assessment Report on Money Laundering and Terrorist Financing (NRA II), 2025.
2. Digital Economy and Business Committee, Cambodia Financial Technology Development Policy 2023-2028, Cambodia: 2023.
3. Robby Houben, Alexander Snyers, Crypto-assets: Key developments, regulatory concerns and responses, Luxembourg: European Parliament, 2020.
4. FATF, International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation: The FATF Recommendations, Paris: 2025.
5. KAS, Law Brief 2.0: Digital Law, Cambodia: 2024.
6. Basel Committee on Banking Supervision, Core Principles for effective banking supervision, 2024.
7. Dubai Virtual Assets Regulatory Authority, Technology and Information Rulebook, Dubai: 2025.
8. EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019.

#### Websites

1. Chainalysis Team, "The 2025 Global Adoption Index: India and the United States Lead Cryptocurrency Adoption," Chainalysis, September 2, 2025, <https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/>
2. Tareq Sikder, "Coinbase, Binance Among 16 Crypto Exchange Websites Blocked by Cambodia," Finance Magnates, December 04, 2024, <https://www.financemagnates.com/cryptocurrency/coinbase-binance-among-16-crypto-exchange-websites-blocked-by-cambodia/>
3. Brandon Tan Jun Wen, "The Flawed Approach of Cambodia's Cryptocurrency Ban," Fulcrum Analysis of Southeast Asia, January 9, 2025, <https://fulcrum.sg/the-flawed-approach-of-cambodias-cryptocurrency-ban/>
4. "Coinbase Singapore Pte. Ltd." Monetary Authority of Singapore, <https://eservices.mas.gov.sg/fid/institution/detail/235467-COINBASE-SINGAPORE-PTE-LTD>
5. "OKX SG Pte. Ltd." Monetary Authority of Singapore, <https://eservices.mas.gov.sg/fid/institution/detail/422854-OKX-SG-PTE-LTD>
6. Lockridge Okoth, "Kraken Wins Major License in Dubai, Binance and OKX to Face New Competition", Yahoo Finance, 21 May 2026, <https://finance.yahoo.com/markets/crypto/articles/kraken-wins-major-license-dubai>
7. "Regulatory Sandbox", Financial Conduct Authority, March 06, 2026, <https://www.fca.org.uk/firms/innovation/regulatory-sandbox>



**PART IV**  
**ARTIFICIAL INTELLIGENCE,**  
**DATA AND LAW**







## Abstract

Despite the rapid advancement of artificial intelligence (AI), Cambodian copyright law does not clearly address the use of copyrighted works in AI training for educational purposes. In particular, the existing legal framework lacks a clear definition of educational use and provides no guidance on how copyright exceptions apply to AI training activities. This legal uncertainty creates challenges for authors, copyright holders, AI developers, and educational institutions.

This brief examines the applicability of Articles 21 and 25 of the Cambodian Law on Copyright and Related Rights to AI training in educational contexts. To address this issue, the brief adopts a comparative approach by drawing on scholarly analysis and United States jurisprudence, where courts have already confronted copyright issues arising from AI training. While these comparative sources are not legally binding in Cambodia, they provide valuable insights for understanding the relationship between AI, educational use, and reproduction rights.

The analysis finds that the current Cambodian framework is insufficient to address the technological realities of AI training and that the absence of clear guidance may lead to inconsistent interpretations and legal uncertainty. Accordingly, this brief argues that Cambodia should clarify the scope of educational use under Article 25 and develop specific rules governing AI training, particularly by distinguishing between non-commercial educational or research activities and commercial AI deployment. Such reforms would provide greater legal certainty while balancing technological innovation, access to education, and the protection of authors' rights.

## I. Introduction

The swift advancement of the digitalization system, particularly the Artificial Intelligence (AI), has transformed education through AI-assisted tutoring, automated content creation, and data-driven research. These technologies rely on large volumes of data, including copyrighted works, giving rise to new challenges for copyright law. As AI systems increasingly use copyrighted materials for training, questions arise as to whether existing copyright frameworks, originally designed for human use, are capable of regulating machine-driven processes while maintaining an appropriate balance between access to education and the protection of authors' rights.

As a Least Developed Country (LDC) under the World Trade Organization (WTO), Cambodia benefits from additional flexibility until 2034 to develop its intellectual property framework. This provides an opportunity to modernize its copyright regime in response to emerging technologies such as AI. Nevertheless, it also highlights the need to clarify the application of existing copyright provisions to AI-related activities.

In Cambodia, Law on Copyright and Related Rights (2003) offers an exception for educational purposes under Article 25<sup>1</sup>, permitting certain unauthorized uses of copyrighted works when non-commercial and properly attributed. While this promotes education and access to knowledge, it was enacted before AI and digital learning technologies, therefore it does not explicitly address the use of copyrighted works in AI systems, such as data training, automated content generation, and large-scale analysis.

Existing scholars reveal a significant divide on how AI training should be treated under copyright law. Some scholars argue that AI training is analogous to human learning and should be considered a transformative and socially beneficial use, especially when it supports research and education<sup>2</sup>. Others, however, emphasize that AI training involves large-scale reproduction of copyrighted works and may generate outputs that compete with original works, thereby undermining authors' economic rights<sup>3</sup>. These competing views are reflected in several United States cases addressing fair use, educational use, and reproduction rights in the context of AI training. Accordingly, this brief relies on the analysis of these scholars and the jurisprudence of the U.S., which is home to many leading AI companies and has actively addresses the AI-related copyright issues, as a comparative foundation for analysis. Given the limited legal framework and absence of domestic jurisprudence concerning AI and copyright in Cambodia, these comparative approaches provide a valuable foundation from which Cambodia may draw guidance in developing future legal and regulatory responses to AI-related copyright challenges.

1 Law on Copyright and Related Rights, February 13, 2003, NS/RKM/0303/008 (Kh.), Article 25.

2 Jenny Quang, "Does Training AI Violate Copyright Law?," Berkeley Technology Law Journal 36, no.4 (2021), p.1408-1436; Christophe Geiger, Francesca Di Lazzaro, "Sustainability as a Guiding Principle for Copyright Reform: Regulating the Use of Generative AI in the Field of Research and Education," Innovation Law and Ethics Observatory Research Paper Series No. 25-02, (Spring 2025), p.1-13; Stuart D. Levi, Mana Ghaemmaghami, MacKinzie M. Neal, "Copyright Office Weighs In on AI Training and Fair Use," Skadden, Arps, Slate, Meagher & Flom LLP, New York, Memorandum, 2025, p.2-4; Edward Lee, "Fair Use and the Origin of AI Training", Santa Clara University School of Law (2025), p.101-223.

3 Sebastian Stober, Tim W. Dornis, "Generative AI Training and Copyright Law," Transactions of the International Society for Music Information Retrieval, (2026), p.6; Shikhar Gupta, "Intellectual Property Rights in AI-Created Educational Content: Issues and Solutions," Educational Administration: Theory and Practice 30(1) (2024), p.6903.

This law brief evaluates the adequacy of the Law on Copyright and Related Rights (2003) in regulating AI-driven educational use in Cambodia. It assesses whether AI training using copyrighted works falls within the education exception under Article 25 or constitutes reproduction requiring authorization under Article 21. The brief aims to clarify the current legal framework's limitations and identify areas where it fails to address contemporary technological realities.

his brief conducts a structured analysis of the issues at hand. It begins by exploring the scope and limitations of Cambodian law concerning the permitted use of copyright for educational purposes (II). The analysis then considers the extent of reproduction involved in AI training and its impact on the author's exclusive rights (III). Next, it examines whether AI training using copyrighted works is permitted as educational use (IV). Additionally, the brief concludes by assessing the overall adequacy of the current legal provisions under Cambodian law and recommendations for the response to emerging technologies and the balancing between educational fair use and author copyright protection (V).

## **II. Scope and Limitations of Cambodian Law Concerning the Permitted Use of Copyright for Educational Purposes**

Article 25 of Cambodian copyright law permits the use of copyrighted works for educational purposes without authorization, provided it's not for financial gain. This reflects the policy of promoting knowledge access and supporting education. However, it is a limited exception to copyright protection. Article 21 grants authors exclusive rights to reproduce, share, and distribute their works, ensuring they control and profit from them. The relationship between these articles is crucial as Article 25 supports educational access, while Article 21 ensures this exception does not interfere with authors' economic interests. Despite this, the context of digital and AI technologies creates challenges in maintaining the balance.

Article 25(c) explicitly stated that "the author cannot prohibit the use of work for the purposes of education, which is not for financial gain". However, the term "educational purpose" is not clearly defined or elaborated, creating uncertainty about its application to modern digital and online education. While it emphasizes that educational use won't be for financial gain, practical implementation raises questions since educational institutions charge fees and some digital learning platforms operate on subscription-based models. This raises the question of whether such activities fall within the exception.

Provisions like Article 24, 27, 28, and 29 address permitted reproduction of copyrighted works, allowing for temporary reproduction in favour of the owner or mentioning authors for research and educational use. However, these provisions do not specify the extent of permissible use, such as how much work may be reproduced or shared in educational use with regard to digital environments. This lack of quantitative limits creates a blurred implication, especially when copying and dissemination can occur on a large scale.

Although both interpretations present valid points, Cambodian law lacks a method to resolve the conflict between innovation and copyright protection. Unlike countries like the United States (U.S.), Cambodia has not implemented a specific exception for text and data mining. As a result, using general copyright rules leads to legal uncertainty for AI developers and copyright owners. A potential remedy could involve establishing a limited exception for text and data mining for non-commercial research and educational institutions, along with licensing requirements for commercial AI training. This strategy would maintain innovation incentives while protecting authors' economic rights.

## **III. The Ambiguity Surrounding the Extent of Reproduction in Artificial Intelligence Training and Its Impact on Authors' Rights**

AI training requires machine learning systems to ingest, copy, store, and process vast quantities of data, including copyrighted works<sup>4</sup>. This raises significant legal concerns under Article 21 of the Cambodia Law on Copyright and Related Rights, which grants authors the exclusive right to reproduce their works.

Two primary and contrasting interpretations have emerged regarding this issue. The first interpretation views AI training as involving non-expressive and intermediate copying, which should not be considered copyright infringement. "Non-expressive use" refers to uses that involve copying, but don't communicate the expressive aspects of the work to be read or otherwise enjoyed<sup>5</sup>.

<sup>4</sup> Jenny Quang, "Does Training AI Violate Copyright Law?" op.cit., p.1410; Stuart D. Levi, Mana Ghaemmaghami, MacKinzie M. Neal, "Copyright Office Weighs in on AI Training and Fair Use," op.cit., p.2; Patrick Gallaher, "Piracy vs. Fair Use: How AI Training Intersects with Copyright Law," Public Knowledge, September 16, 2025, <https://publicknowledge.org/piracy-vs-fair-use-how-ai-training-intersects-with-copyright-law/>, p.3.

<sup>5</sup> Authors Alliance, "Why Fair Use Supports Non-Expressive Use?" February 29, 2024, <https://www.authorsalliance.org/2024/02/29/why-fair-use-supports-non-expressive-uses/>.



Scholars like Jenny Quang argue that while AI training necessitates extensive downloading, storage, and data mining, these activities are merely technical and non-communicative uses of copyrighted works. According to this perspective, “not all copying constitutes copyright infringement<sup>6</sup>.” Quang draws on *Baker v. Selden* to illustrate the distinction between a copyrighted work and its material form. In that case, Selden obtained copyright protection over a book explaining a novel accounting system, including accounting forms used to demonstrate the system<sup>7</sup>. Later, Baker adopted a similar accounting system and reproduced comparable forms in practice. The Court ruled that copyright protected the explanatory expression contained in the book, but not the underlying accounting method itself, which rightfully belonged within the domain of patent law. Consequently, Baker was not held liable because he used the forms functionally rather than expressively<sup>8</sup>.

Building upon this reasoning, proponents of the non-expressive use theory contend that AI training does not exploit copyrighted works for their expressive purpose but rather extracts patterns, statistical relationships, and functional information. Since the training data is not directly shared with the public, they argue that the process does not interfere with the expressive value of the works and therefore should not constitute infringement. Under this interpretation, mandating authorization or licensing for every use of copyrighted material in training would be an excessive extension of authors’ rights<sup>9</sup>.

OpenAI has presented a similar perspective, asserting that intermediate copying during AI training is inherently non-expressive and primarily serves to facilitate models’ learning of statistical patterns rather than conveying expressive content to users. According to this argument, each individual work contributes minimally to the resulting system, resulting in minimal or no loss of audience to the original author<sup>10</sup>. Similarly, Patrick contends that while training necessitates temporary copies of works, the resulting AI model fundamentally represents statistical data rather than a direct reproduction of the copyrighted works themselves. Since AI systems process data through computational analysis rather than traditional dissemination of copyrighted works, proponents characterize AI training as a socially advantageous and technologically functional activity that should not infringe upon the author’s exclusive rights<sup>11</sup>.

In contrast, the second interpretation adopts a more rights-protective approach and argues that AI training constitutes *prima facie* infringement of the reproduction right. This view emphasizes that the act of copying itself regardless of its purpose is sufficient to engage the author’s exclusive rights under copyright law. Scholars such as Christophe Geiger and Francesca Di Lazzaro acknowledge that the use of protected works in AI training raises serious concerns regarding authors’ control, recognition, and economic interests. They therefore advocate for a sustainable legal framework capable of protecting both the economic and moral rights of authors in the context of AI development<sup>12</sup>.

Similarly, the United States Copyright Office has stated that the use of copyrighted works in AI training may constitute “*prima facie* infringement” of the reproduction right. According to the report, infringement may occur both from downloading and storing copyrighted works and from making intermediate copies during AI training. It also tackles the debate over “memorization,” questioning if a model’s internal weights are infringing copies. AI developers say these weights are just numbers, but critics argue that similar outputs to training data show copyrighted content is still in the model. The report suggests that if outputs closely match original works, it strongly indicates infringement of reproduction and derivative work rights. It compares AI models to compressed files, where copyrighted content is hidden but still present<sup>13</sup>.

This concern is further supported by Sebastian Stober and Tim W. Dornis, who argue that generative AI differs from traditional text and data mining because it uses expressive elements of copyrighted works to create competing content. They warn that memorization of copyrighted material in AI systems poses an independent risk of unlawful reproduction. They believe that whether humans can interpret the encoded information within the model is irrelevant. What matters is that copyrighted content remains embedded in the system, similar to information on a compact disc or ancient manuscript. Consequently, reproducing or distributing AI models with memorized copyrighted material may infringe copyright, even if the underlying works were lawfully obtained<sup>14</sup>. This systematic copying conflicts with the economic interests protected by copyright law.

6 Jenny Quang, “Does Training AI Violate Copyright Law?” op.cit., p.1419

7 *Baker v. Selden*, 101 U.S. 99 (1879)

8 Jenny Quang, “Does Training AI Violate Copyright Law?” op.cit., p.1419

9 Jenny Quang, “Does Training AI Violate Copyright Law?” op.cit., p.1409

10 Comment Regarding Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation: Comment of OpenAI, LP Addressing Question 3, United States Patent and Trademark Office (.gov), May 11, 2026, [https://www.uspto.gov/sites/default/files/documents/OpenAI\\_RFC-84-FR-58141.pdf](https://www.uspto.gov/sites/default/files/documents/OpenAI_RFC-84-FR-58141.pdf), p.5&7.

11 Patrick Gallaher, “Piracy vs. Fair Use: How AI Training Intersects with Copyright Law,” op.cit., p.2

12 Christophe Geiger, Francesca Di Lazzaro, “Sustainability as a Guiding Principle for Copyright Reform: Regulating the Use of Generative AI in the Field of Research and Education,” op.cit., p.8

13 Stuart D. Levi, Mana Ghaemmaghami, MacKinzie M. Neal, “Copyright Office Weighs in on AI Training and Fair Use,” op.cit., p.3

14 Sebastian Stober, Tim W. Dornis, “Generative AI Training and Copyright Law,” op.cit., p.7&9

When these competing interpretations are considered together, the second approach appears more consistent with the structure and underlying objectives of copyright law. Article 21 clearly establishes reproduction as an exclusive right of the author, and any limitation or exception to that right should therefore be expressly provided and interpreted narrowly. The argument that AI training involves merely “technical” copying is insufficient to remove such activities from the scope of reproduction, as copyright law generally does not distinguish between expressive and non-expressive copying at the infringement stage. Moreover, the scale, permanence, and comprehensiveness of copying involved in AI training distinguish it from more limited intermediate uses, such as temporary caching or incidental technological processes.

Given the potential for AI systems to reproduce, approximate, or compete with protected works, recognizing such copying as entirely non-infringing would risk substantially weakening the protection afforded to authors under copyright law. Accordingly, AI training should be understood as engaging the reproduction right under Article 21, and its legality should depend upon the existence of a clear and applicable statutory exception or authorization framework.

Nevertheless, not all AI training reproduction poses the same risk to authors. Temporary copies for internal use and inaccessible to the public may cause minimal market harm. Some scholars argue that AI innovation’s social and economic benefits justify flexible reproduction rights in limited contexts. An overly rigid copyright law may hinder technological and educational development. A balanced solution may involve specific exceptions, compulsory licensing, or text and data mining frameworks that ensure fair compensation while allowing responsible innovation.

#### **IV. Artificial Intelligence Training Using Copyrighted Works and Permitted Educational Use/Fair Use**

The educational exception under Article 25 permits the use of copyrighted works for non-commercial education purposes. However, the provision lacks a clear definition of the term “educational use” or clarify whether technologically mediated activities such as AI training fall within its application. This ambiguity is understandable given that the legislation was enacted prior to the emergence of modern AI systems capable of processing vast quantities of copyrighted material autonomously<sup>15</sup>. Although the exception was intended to balance copyright protection against the public interest in access to education, the application of that balance becomes increasingly contested when educational activities are conducted through automated computational systems rather than direct human instruction. Without more specific guidance, uncertainty remains as to whether AI training falls within the intended scope of educational use. Accordingly, the central issue is whether such technological use of copyrighted materials can reasonably be equated with the traditional forms of educational use originally contemplated by the law.

Although Cambodian copyright law does not adopt the U.S. fair use doctrine, comparative fair use analysis helps assess educational exceptions for emerging technologies like AI. Unlike the U.S., Cambodia permits only specific exceptions, hence the U.S. flexibility balancing approach cannot be directly applied. However, U.S. cases illustrate how courts balance copyright protection with technological innovation and educational access in AI training, providing valuable guidance for evaluating Article 25 and legal reforms in Cambodia.

Several scholars have referred to the four-factor fair use doctrine, codified under 17 U.S.C. § 107 and commonly applied by United States courts, in addressing the issue of educational use in the context of AI training. The doctrine considers:

1. “the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;”
2. “the nature of the copyrighted work;”
3. “the amount and substantiality of the portion used in relation to the copyrighted work as a whole;” and
4. “the effect of the use upon the potential market for or value of the copyrighted work<sup>16</sup>.”

Two principal competing views have emerged regarding the application of these factors to AI training. The first adopts a broad and functional interpretation of educational use, primarily emphasizing the first factor of fair use. Under this approach, scholars and courts focus on the transformative nature and purpose of the use.

15 Shikhar Gupta, “Intellectual Property Rights in AI-Created Educational Content: Issues and Solutions,” op.cit., p.1; Christophe Geiger, Francesca Di Lazzaro, “Sustainability as a Guiding Principle for Copyright Reform: Regulating the Use of Generative AI in the Field of Research and Education,” op.cit., p.2; Daniel A. Tysver, “Fair Use and the Training of AI Models on Copyrighted Works,” op.cit., p.2-4; Dr Preet Deep Singh, “Why AI Training on Copyrighted Material Constitutes Fair Use,” (2025): Available at SSRN: <http://dx.doi.org/10.2139/ssrn.5287544>; Edward Lee, “Fair Use and the Origin of AI Training,” op.cit., pp.146&156; Jenny Quang, “Does Training AI Violate Copyright Law?,” op.cit., pp.1410-1412

16 U.S.C. §107; Jenny Quang, “Does Training AI Violate Copyright Law?” op.cit., p.1417; Sebastian Stober, Tim W. Dornis, “Generative AI Training and Copyright Law,” op.cit., p.3

They argue that large-scale use of copyrighted works may be permissible where the purpose is not to reproduce the works themselves, but rather to transform them into functional learning tools.

For instance, Jenny Quang states that AI training extracts unprotectable ideas, patterns, and statistical relationships from copyrighted materials in order to build functional systems. According to this view, AI training should be regarded as a technical process that generates social utility, even when the resulting product is ultimately commercial in nature<sup>17</sup>. Similarly, the United States Copyright Office has suggested in its report that educational or “non-commercial research” uses that do not reproduce original copyrighted works in their outputs are more likely to qualify as fair use<sup>18</sup>. Likewise, Edward Lee traces the development of AI training practices to university-based research, where researchers discovered that scaling AI systems through diverse datasets contributed significantly to technological advancement<sup>19</sup>. He emphasizes that such research-oriented AI training serves a legitimate fair use purpose grounded in scientific research and technological innovation<sup>20</sup>.

This functional and transformative approach has also been reflected in United States case law. In *Perfect 10, Inc. v. Amazon.com, Inc.*, the Ninth Circuit held that the use of copyrighted images in a search engine constituted fair use because the thumbnails served a transformative function<sup>21</sup>. While the original images were created for “entertainment, aesthetic, or informative” purposes, the search engine repurposed them as “pointers” directing users to sources of information<sup>22</sup>. Similarly, in *Authors Guild, Inc. v. Google, Inc.*, the Second Circuit found Google’s digitization of copyrighted books to be fair use because the Google Books search engine was highly transformative. The court considered the Google Books project highly transformative<sup>23</sup> because it enabled users to locate relevant information without substituting for the original books<sup>24</sup>.

In contrast, the second approach adopts a narrower and more traditional interpretation of educational use. Proponents of this view contend that the term “educational use” was originally intended to encompass direct and limited uses of copyrighted works, such as classroom instruction, illustration, commentary, or examination purposes, rather than large-scale automated data processing for AI training.

For example, Stober and Dornis acknowledge that fair use traditionally favours activities such as research, education, criticism, and commentary<sup>25</sup>. However, they believe that generative AI training fundamentally differs from traditional text and data mining because it relies extensively on expressive elements of copyrighted works to generate outputs capable of substituting for human-created content. Consequently, they consider reliance on educational exceptions in the context of AI training to be legally uncertain and conceptually weak<sup>26</sup>. Similarly, Shikhar Gupta focuses on the outputs generated by AI systems, particularly in educational contexts. He observes that AI is increasingly used to produce tailored educational materials, including lecture slides, syllabi, and assessment tools<sup>27</sup>. Although these uses may appear transformative, Gupta suggests that they create a legal complex concerning questions of ownership and authorship between educators, institutions, and AI developers<sup>28</sup>.

A comparable perspective is reflected in analyses of *Bartz v. Anthropic*. In that case, the Court acknowledged some interim victories for the AI industry. Judge William Alsup found Anthropic’s use of copyrighted works to train its AI model “exceedingly transformative,” favouring fair use. He also ruled that digitizing lawfully purchased books for training did not constitute infringement. However, the court distinguished this from Anthropic’s downloading and storing pirated works, which could lead to liability. Despite treating piracy and AI training as separate acts, the decision showed that transformative purpose does not excuse unlawful access to copyrighted material<sup>29</sup>.

These criticisms collectively emphasize that AI training differs fundamentally from traditional educational activities because it lacks direct educational interaction and operates through automated computational processes.

17 Jenny Quang, “Does Training AI Violate Copyright Law?” op.cit., p.1417

18 Stuart D. Levi, Mana Ghaemmaghami, MacKinzie M. Neal, “Copyright Office Weighs in on AI Training and Fair Use,” op.cit., p.2-3.

19 Edward Lee, “Fair Use and the Origin of AI Training”, op.cit., p.101

20 Edward Lee, “Fair Use and the Origin of AI Training”, op.cit., p.112

21 *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, (9th Cir. 2007).

22 *Ibid.*

23 *Authors Guild, Inc. v. Google Inc.*, F.3d 202, 216 (2d Cir. 2015).

24 *Authors Guild, Inc. v. Google Inc.*, 954 F. Supp. 2d 282, 291 (S.D.N.Y. 2013), *aff’d*,

804 F.3d at 202; Jenny Quang, “Does Training AI Violate Copyright Law?” op.cit., p.1417

25 Sebastian Stober, Tim W. Dornis, “Generative AI Training and Copyright Law,” op.cit., p.3

26 Sebastian Stober, Tim W. Dornis, “Generative AI Training and Copyright Law,” op.cit., p.6

27 Shikhar Gupta, “Intellectual Property Rights in AI-Created Educational Content: Issues and Solutions,” op.cit., pp.6903-6904

28 Shikhar Gupta, “Intellectual Property Rights in AI-Created Educational Content: Issues and Solutions,” op.cit., p.6899

29 Sebastian Stober, Tim W. Dornis, “Generative AI Training and Copyright Law,” op.cit., pp.2-3

Ultimately, the second, narrower interpretation appears more persuasive and legally sound. Although AI training may pursue educational objectives, the classification of a use should depend not only on its intended purpose, but also on its nature, scale, and impact on the rights of copyright holders. Article 25 constitutes a limited exception to the author's exclusive rights and, as such, should be interpreted restrictively. AI training extends beyond the limited and purpose-specific educational activities traditionally contemplated under Article 25.

Moreover, equating AI training with human learning overlooks the fundamental differences between the two processes. Unlike human learners, AI systems rely on automated, large-scale computational processing of copyrighted works, which extends beyond the traditional educational activities contemplated by Article 25. Permitting AI training under the educational exception without further clarification could therefore expand the scope of the provision beyond its original legislative intent.

Nevertheless, a broad exclusion of AI training may also be overly restrictive. AI training conducted by non-profit academic institutions for research purposes, or training designed to avoid reproducing expressive elements of copyrighted works, may pose a lower risk to authors' interests. As noted by Preet Deep Singh, AI training transforms copyrighted works into non-expressive statistical patterns, suggesting that the resulting outputs are not direct copies of the original works<sup>30</sup>. Accordingly, a more balanced approach would distinguish between non-commercial research-oriented AI training and commercial AI deployment, thereby promoting educational and technological innovation while safeguarding authors' economic rights.

## V. Implications for Cambodian Copyright Law

The analysis reveals that the Cambodian Law on Copyright and Related Rights is currently limited in addressing the challenges posed by AI training in educational settings. While Articles 21 and 25 offer a general framework for reproduction rights and educational exceptions, these provisions were enacted before the creation of modern AI technologies. Consequently, they do not adequately address the large-scale and automated use of copyrighted works by AI systems.

Several regulatory gaps remain. First, Article 25 does not define the scope of "educational use" or clarify whether AI training falls within the exception. Second, Cambodian copyright law does not provide a specific exception for text and data mining, despite its fundamental role in AI training. Third, there are no AI-specific provisions or administrative guidelines governing the application of copyright law to AI-related activities. Finally, the absence of domestic jurisprudence further contributes to legal uncertainty for copyright holders, educational institutions, and AI developers.

These gaps create practical and legal challenges. Educational institutions and researchers may be uncertain whether AI-assisted teaching and research are permissible under Article 25, while AI developers face uncertainty regarding potential copyright liability. At the same time, authors risk the unauthorized large-scale use of their works without adequate safeguards or compensation. Such uncertainty may hinder both technological innovation and the effective protection of authors' rights.

Accordingly, Cambodia should consider modernizing its copyright framework. This may include clarifying the meaning of "educational use" under Article 25, introducing a limited text and data mining exception for non-commercial research and educational purposes, and distinguishing between non-commercial AI training and commercial AI deployment, with the latter subject to appropriate authorization or licensing requirements. In the interim, relevant authorities could issue interpretative guidelines to provide greater legal certainty until comprehensive legislative reforms are enacted.

By adopting these measures, Cambodia would be better positioned to balance technological innovation, access to education, and the protection of authors' rights in an increasingly AI-driven environment.

## VI. Conclusion

In conclusion, this brief has argued that Article 25 of the Cambodian Law on Copyright and Related Rights is not yet sufficient to regulate the use of copyrighted works in AI systems for educational purposes. Enacted in a pre-digital context, the provision does not adequately address AI training or automated data processing, resulting in uncertainty as to whether such activities fall within the scope of "educational use" under Article 25 and whether they engage the reproduction rights protected under Article 21.

While certain forms of non-profit, research-oriented AI training may align with the rationale underlying educational use, the large-scale and automated nature of AI training distinguishes it from the traditional

educational activities contemplated by the law. Extending the educational exception to AI training without legislative clarification therefore risks undermining authors' economic rights.

Accordingly, Cambodia should modernize its copyright framework by clarifying the scope of educational use, introducing appropriate rules on text and data mining, and providing guidance on the application of copyright law to AI-related activities. Such reforms would promote legal certainty while balancing technological innovation, access to education, and the protection of authors' rights.



## Bibliography

### Legislations

1. Law on Copyright and Related Rights, February 13, 2003, NS/RKM/0303/008 (Kh.), [https://data.open-developmentcambodia.net/laws\\_record/law-on-copy-rights-and-related-rights](https://data.open-developmentcambodia.net/laws_record/law-on-copy-rights-and-related-rights)

### Journal Articles

1. Christophe Geiger, Francesca Di Lazzaro, "Sustainability as a Guiding Principle for Copyright Reform: Regulating the Use of Generative AI in the Field of Research and Education," Innovation Law and Ethics Observatory Research Paper Series No. 25-02, Spring 2025: pp.1-13. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5191571](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5191571)
2. Dr Preet Deep Singh, "Why AI Training on Copyrighted Material Constitutes Fair Use," (2025): Available at SSRN: <http://dx.doi.org/10.2139/ssrn.5287544>
3. Edward Lee, "Fair Use and the Origin of AI Training", Santa Clara University School of Law (2025): pp.1 01-223. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5253011](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5253011).
4. Jenny Quang, "Does Training AI Violate Copyright Law?" Berkeley Technology Law Journal 36, no.4 (2021): pp.1408-1435. <https://lawcat.berkeley.edu/record/1253129?v=pdf>
5. Sebastian Stober, Tim W. Dornis, "Generative AI Training and Copyright Law," Transactions of the international Society for Music Information Retrieval, (2026): pp.1-16. <https://arxiv.org/abs/2502.15858>.
6. Shikhar Gupta, "Intellectual Property Rights in AI-Created Educational Content: Issues and Solutions," Educational Administration: Theory and Practice 30(1) (2024): pp.6895-6907. <https://doi.org/10.53555/kuey.v30i1.10139>
7. Yotam Werzansky-Orland, "Artificial Intelligence and Copyright Protection: AI-generated content and question of copyright," International Journal of Business 5, (2024): pp.1-20.[https://www.researchgate.net/publication/381566789\\_AI-Generated\\_Content\\_and\\_the\\_Question\\_of\\_Copyright](https://www.researchgate.net/publication/381566789_AI-Generated_Content_and_the_Question_of_Copyright).

### Reports

1. Comment Regarding Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation: Comment of OpenAI, LP Addressing Question 3, United States Patent and Trademark Office (.gov), May 11, 2026, [https://www.uspto.gov/sites/default/files/documents/OpenAI\\_RFC-84-FR-58141.pdf](https://www.uspto.gov/sites/default/files/documents/OpenAI_RFC-84-FR-58141.pdf).
2. Daniel A. Tysver, "Fair Use and the Training of AI Models on Copyrighted Works," BitLaw, May 6, 2026, <https://www.bitlaw.com/ai/AI-training-fair-use.html>.
3. Stuart D. Levi, Mana Ghaemmaghami, MacKinzie M. Neal, "Copyright Office Weighs In on AI Training and Fair Use," Skadden, Arps, Slate, Meagher & Flom LLP, New York, Memorandum, 2025. <https://www.skadden.com/insights/publications/2025/05/copyright-office-report>.
4. Zirpoli, Christopher T., Law, "Constitution & Civil Liberties; Science & Technology," Congress.Gov, July 18, 2025, <https://www.congress.gov/crs-product/LSB10922?hl=Generative+Artificial+Intelligence+and+Copyright+Law&s=1&r=2>.

### News Articles

12. Hughstephensblog, "Why 'Fair Use' Cannot Justify Piracy in AI Training Case," Hughstrphensblog: Insights on International Copyright Issue, September 13, 2025, <https://hughstephensblog.net/2025/09/13/when-the-end-does-not-justify-the-means-anthropics-1-5-billion-lesson/>.
13. Patrick Gallaher, "Piracy vs. Fair Use: How AI Training Intersects with Copyright Law," Public Knowledge, September 16, 2025, <https://publicknowledge.org/piracy-vs-fair-use-how-ai-training-intersects-with-copy-right-law/>.



## **The Legal Status of Synthetic Data under Cambodian Law Where Re-Identification Is Reasonably Possible**

*HAY Sarkunmealea*

## Abstract

The increasing use of synthetic data in healthcare, finance, and technology presents new challenges for data protection law, particularly where such data may still permit the re-identification of individuals. This law brief examines whether synthetic data should be treated as personal data under Cambodian law when re-identification remains reasonably possible. It analyses the existing legal framework, focusing primarily on Article 32 of the Law on Electronic Commerce and Article 65(b) of the Law on Telecommunications, both of which provide privacy protections but do not define the legal status of synthetic data or establish a standard for assessing re-identification risks. The brief argues that this legislative gap creates significant uncertainty regarding accountability, liability, and regulatory compliance when synthetic datasets are generated, shared, or transferred. It evaluates three possible approaches to classification: categorical exclusion, categorical inclusion, and a risk-based approach based on the likelihood of re-identification. After assessing the strengths and limitations of each approach, the brief concludes that a risk-based classification best reflects the protective purpose of Cambodian data protection law while maintaining proportionality between privacy protection and technological innovation. It recommends that Cambodia explicitly recognize re-identification risk as the determining factor for the legal treatment of synthetic data to provide greater certainty for regulators, organizations, and individuals.

## I. Introduction

A hospital generates a synthetic patient dataset and transfers it abroad without consent and without applying the security safeguards in Article 32 of the Law on Electronic Commerce (“E-commerce”) that would be required for personal information held in electronic form<sup>1</sup>. Whether this conduct falls within that obligation depends on the question of whether synthetic data, namely data generated by a computational model trained on real personal records, constitutes the kind of information that Article 32 protects.

According to the Law on E-commerce, any person holding personal information in electronic form must use all reasonable means to protect that information against loss, unauthorized access, alteration, or disclosure<sup>2</sup>. The obligation in Article 32 is framed by reference to personal information, a term the Law on E-commerce does not itself define with a general identifiability test, leaving open whether information generated by a model, rather than directly recorded, falls within its scope<sup>3</sup>. Cambodia’s Law on Telecommunications separately preserves a subscriber’s right to privacy, security, and safety in the use of telecommunications services, a right that attaches to the subscriber relationship rather than to any defined category of data<sup>4</sup>. That right is also qualified by an exception clause permitting derogation where otherwise determined by other specific laws, which means the protection it affords depends on legal categorization elsewhere in Cambodian law, categorization that does not currently address synthetic data<sup>5</sup>.

Synthetic data complicates this framework because it occupies an intermediate position relative to the categories these provisions assume. It contains no name, no subscriber number, and no record that corresponds one-to-one with a real person, which might suggest it falls outside Article 32’s reference to personal information. Yet it is generated by training a computational model on real personal records, and the model may retain statistical patterns specific enough to allow a source individual to be identified again, which would bring it within the kind of information Article 32 was designed to protect<sup>6</sup>.

This raises a more general question: should classification under Article 32, and under the privacy guarantee in Article 65(b) of the Law on Telecommunications, depend on the form a dataset takes, meaning whether it contains direct identifiers, or on the risk it poses to identifiable individuals, meaning whether those individuals can still be found within it through indirect means. The absence of a clear answer raises a fundamental question: should synthetic data be treated as personal data where re-identification remains reasonably possible. This brief, therefore, proceeds in three parts. First, it examines the legal status of synthetic data under Cambodian law by analyzing the current protection of personal information and the limitations of existing rules in addressing re-identification risks. Second, it considers the consequences of legal uncertainty, particularly with respect to accountability, liability, and regulatory compliance. Finally, it evaluates the competing approaches to the legal classification of synthetic data and considers which approach is most consistent with the structure and purpose of Cambodian law.

1 Kingdom of Cambodia, Law on Electronic Commerce, Royal Kram No. NS/RKM/1119/017 (2019), art. 32.1.

2 Law on Electronic Commerce, op. cit., art. 32.1.

3 Law on Electronic Commerce, op. cit., art. 4.

4 Kingdom of Cambodia, Law on Telecommunications, Royal Kram No. NS/RKM/1215/017 (2015), art. 65(b).

5 Cambodian Center for Human Rights, “*Cambodia’s Law on Telecommunications: A Legal Analysis*” (Phnom Penh: LICADHO, March 2016), [https://www.licadho-cambodia.org/reports/files/214LICADHOTElecomsLawLegalAnalysis\\_March-2016ENG.pdf](https://www.licadho-cambodia.org/reports/files/214LICADHOTElecomsLawLegalAnalysis_March-2016ENG.pdf), pp. 4-6.

6 Theresa Stadler, Bristena Oprisanu, and Carmela Troncoso, “*Synthetic Data -- Anonymisation Groundhog Day*,” Proceedings of the 31st USENIX Security Symposium (2022), <https://www.usenix.org/conference/usenixsecurity22/presentation/stadler>, pp. 1451-1467.

This brief proceeds from a simple proposition: synthetic data is not personal in form, but it may remain personal in risk. Resolving the tension between these two ideas is increasingly relevant as synthetic data becomes more widely used across Cambodia's healthcare, banking, and technology sectors.

## II. The Legal Status of Synthetic Data Under Cambodian Law

### A. Existing Protection of Personal Information under Cambodian Law

Article 32 of the Law on Electronic Commerce provides that any person who holds personal information in electronic form must use all reasonable means to ensure that the information is protected by security safeguards appropriate to the sensitivity of the information, and prohibits the use of another person's data for any purpose without authorization<sup>7</sup>. This is the closest provision Cambodian law has to a general data protection rule, but its scope depends on what counts as personal information, a term the Act does not define by reference to identifiability, whether direct or indirect.

Article 65(b) of the Law on Telecommunications preserves a telecommunications subscriber's right to privacy, security, and safety in the use of telecommunications services<sup>8</sup>. This right is expressly subject to derogation where otherwise determined by other specific laws, a qualification that has drawn sustained criticism for undermining the protection it appears to grant<sup>9</sup>. The right attaches to the subscriber relationship between an operator and a subscriber; it does not articulate a general standard for determining when other forms of information, including information generated by a computational process rather than collected directly from a subscriber, fall within its scope.

Beyond these two instruments, matters of personal data and privacy in Cambodia are addressed only indirectly, through the constitutional guarantee in Article 40, which protects the secrecy of correspondence by mail, telegram, fax, telex, and telephone, and through provisions of the Civil Code recognizing privacy as a personal right<sup>10</sup>. None of these instruments was drafted with artificially generated data in mind, and none addresses the question of indirect identifiability with the specificity that synthetic data requires. This reflects the period in which each instrument was enacted, prior to the widespread use of generative computational methods in Cambodia's banking, health, and technology sectors, rather than any considered legislative judgment that such data should fall outside protection.

### B. Absence of Direct Identifiers Excludes Synthetic Data from Protection under the Law

The most direct argument for excluding synthetic data from Article 32 is that it contains no name, no subscriber number, and no record traceable to a specific individual, and personal information, on a narrow reading, means information that directly names or numbers a person. If identifiability is understood this narrowly, the argument succeeds. But identifiability in comparative data protection analysis has more commonly extended to indirect identification, meaning cases where an individual can be singled out through a combination of information even without a name appearing in the dataset<sup>11</sup>.

Synthetic data is generated by training a computational model on real personal records and using that model to produce new records. The model itself encodes statistical relationships present in the training data. Whether those relationships are specific enough to allow a particular source individual to be identified again is a question that depends on the generation method, the size of the training dataset, and the information available to anyone attempting re-identification<sup>12</sup>. These are factual and technical questions. Article 32 does not provide a legal test for resolving them in the context of data that was never directly collected from the individual it may still relate to, which means an organization in Cambodia generating a synthetic dataset has no reliable basis for determining, in advance, whether its dataset would be treated as personal information for the purposes of that Article.

<sup>7</sup> Law on Electronic Commerce, op. cit., arts. 32.1-32.2.

<sup>8</sup> Law on Telecommunications, op. cit., art. 65(b).

<sup>9</sup> Cambodian Center for Human Rights, "Cambodia's Law on Telecommunications: A Legal Analysis," op. cit., [https://www.licadho-cambodia.org/reports/files/214LICADHOTelecomsLawLegalAnalysis\\_March2016ENG.pdf](https://www.licadho-cambodia.org/reports/files/214LICADHOTelecomsLawLegalAnalysis_March2016ENG.pdf), pp. 4-5.

<sup>10</sup> Kingdom of Cambodia, Constitution of the Kingdom of Cambodia (1993, as amended), art. 40; Kingdom of Cambodia, Civil Code (2007), provisions on personal rights.

<sup>11</sup> Paul Schwartz and Daniel Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information," New York University Law Review 86, no. 6 (2011): pp. 1814-1894.

<sup>12</sup> Stadler, Oprisanu, and Troncoso, "Synthetic Data -- Anonymisation Groundhog Day," op. cit., <https://www.usenix.org/conference/usenixsecurity22/presentation/stadler>, pp. 1455-1460.

## C. The Absence of an Anonymisation Standard

A natural response is to treat synthetic data as a form of anonymized data, on the reasoning that data generated artificially, rather than collected directly, has already been sufficiently distanced from any real individual to fall outside Article 32. This response requires a standard for anonymization: a method for determining when the link between a dataset and an identifiable individual has been broken to a degree the law accepts<sup>13</sup>.

Neither the Law on Electronic Commerce nor the Law on Telecommunications articulates such a standard. Article 32 addresses the security of personal information once it is held; it does not address the conditions under which data ceases to relate to an identifiable individual in the first place. In jurisdictions that have addressed this question directly, anonymization has generally not been treated as a fixed technical state but as a conclusion reached after assessing the likelihood of re-identification using the means reasonably available to a person attempting it<sup>14</sup>. The history of anonymization techniques has documented that data once thought to be safely anonymized has, in a number of cases, later been re-identified as additional auxiliary information became available, which suggests that anonymization claims require ongoing scrutiny rather than a one-time technical assessment<sup>15</sup>.

Without an anonymization standard of its own, Cambodian law has no basis on which an organization, a court, or a regulator could test a claim that a particular synthetic dataset falls outside Article 32. The classification question, in this respect, remains open not because Cambodian law has considered the question and reached a particular answer, but because the law has not yet built the tool required to decide it.

## III. The Consequences of Legal Uncertainty

### A. Accountability for Sharing and Transferring Synthetic Data

If synthetic data is treated as falling outside Article 32, an organization holding personal records subject to that Article's security obligation could generate a synthetic dataset from those records and share, transfer, or process the synthetic version without the safeguards that would attach to the underlying personal information. The synthetic dataset may carry much of the practical value of the original data, including the statistical patterns relevant to credit scoring, treatment outcomes, or behavioural prediction, while falling outside the category of information Article 32 protects.

This raises a direct question. If personal information can be converted into a form that escapes the obligation attaching to it under Article 32, without any assessment of whether the resulting data still carries identifiability risk, does that Article continue to serve its protective function with respect to that data? The question is not whether such conversion is technically possible; the technical capability is well documented<sup>16</sup>. The question is whether Cambodian law, as it currently stands, has any means of distinguishing a conversion that genuinely removes identifiability risk from one that does not.

### B. Responsibility for Harm Following Re-Identification

A related question arises where a synthetic dataset is in fact re-identified and a source individual suffers harm as a result, for example through the disclosure of a medical condition or a financial circumstance. If the synthetic dataset was not treated as personal information at the point of generation or transfer, no person was held to the security obligation under Article 32 with respect to it, and no party was subject to the safeguards that provision requires for personal information held in electronic form.

This leaves open the question of who, if anyone, bears responsibility for the resulting harm: the organization that generated the synthetic dataset, the party that carried out the re-identification, or neither, on the basis that the data was never personal information for the purposes of Article 32 to begin with. Technical research on generative models has shown that re-identification of source individuals from synthetic outputs, through methods such as membership inference, is not merely a theoretical possibility but has been demonstrated under realistic conditions<sup>17</sup>. Cambodian law, lacking a classification rule for synthetic data, does not currently

13 Luk Arbuckle and Khaled El Emam, *Building an Anonymization Pipeline: Creating Safe Data* (Sebastopol: O'Reilly Media, 2020), pp. 45-50.

14 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 (2010): pp. 1701-1777.

15 Ohm, "Broken Promises of Privacy," op. cit., pp. 1704-1716.

16 Stadler, Oprisanu, and Troncoso, "Synthetic Data -- Anonymisation Groundhog Day," op. cit., <https://www.usenix.org/conference/usenixsecurity22/presentation/stadler>, pp. 1451-1455.

17 Nicholas Carlini, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Tramer, "Membership Inference Attacks From First Principles," 2022 IEEE Symposium on Security and Privacy, pp. 1897-1914.



provide an answer to who bears responsibility in this scenario, and general principles of civil liability under the Civil Code would face significant practical difficulty establishing the causal chain between the generation of a dataset and a specific re-identification harm without a settled legal starting point for what kind of data was involved.

### **C. Legal Uncertainty and Compliance Challenges**

A further consequence of the unresolved classification question is that organizations seeking to comply with Article 32 in good faith have no reliable basis for assessing their obligations. An organization that wishes to apply protective measures to its synthetic data practices, out of caution or because it operates across multiple jurisdictions, cannot determine from Cambodian law what standard it should meet, since no standard for assessing re-identification risk currently exists under Article 32 or elsewhere.

Regional instruments addressing data governance in Southeast Asia have recognized that the absence of clear classification rules can itself undermine both privacy protection and the development of reliable data practices, since organizations cannot make consistent compliance decisions without a stable reference point<sup>18</sup>. Whatever approach Cambodia eventually adopts, the absence of any approach at present means that compliance with Article 32, enforcement, and dispute resolution involving synthetic data all proceed without a shared legal vocabulary.

## **IV. APPROACHES TO THE CLASSIFICATION OF SYNTHETIC DATA**

### **A. Categorical Exclusion**

One approach treats synthetic data as categorically outside the scope of Article 32, on the basis that it contains no direct identifiers and that subjecting it to the security obligation would impose unnecessary burdens on data-driven activity without a corresponding privacy benefit<sup>19</sup>.

This approach has the advantage of clarity: an organization generating synthetic data would know, without further inquiry, that Article 32 does not apply.

The difficulty with this approach is that it treats the absence of a direct identifier as equivalent to the absence of identifiability, when the two are not the same thing under an indirect-identification standard. A categorical exclusion rule would apply equally to a synthetic dataset carrying negligible re-identification risk and one carrying significant risk, since the rule does not ask the question on which that distinction depends. This means the approach may produce the same outcome under Article 32, namely no obligation at all, regardless of how much identifiability risk a particular synthetic dataset actually carries.

### **B. Categorical Inclusion**

A second approach treats synthetic data as always falling within Article 32's reference to personal information, on the basis that it is generated from real personal records and that the interests the provision protects remain engaged throughout its use, regardless of how the data is subsequently labelled.

This approach has the advantage of removing any incentive to relabel personal information as synthetic in order to avoid the Article 32 obligation, since the obligation would apply either way. Its difficulty is that it would impose the same security safeguard on a synthetic dataset with demonstrably negligible re-identification risk as on a raw database of real records. Where the risk to source individuals is genuinely minimal, this approach may impose burdens not justified by reference to the harm Article 32 is designed to prevent.

### **C. Risk-Based Classification**

A third approach classifies synthetic data as personal information for the purposes of Article 32 only where re-identification of source individuals remains reasonably possible, having regard to the generation method, the characteristics of the training dataset, and the means realistically available to someone attempting re-identification. Under this approach, the organization generating the dataset would bear the task of showing that re-identification<sup>20</sup> is not reasonably possible; where it cannot make that showing, the dataset would be treated as personal information and the Article 32 safeguard would apply.

This approach more closely tracks the apparent purpose of Article 32, which is concerned with protecting information from a risk of harm rather than with the technical process by which the information was pro-

18 ASEAN Secretariat, ASEAN Data Management Framework (Jakarta: ASEAN, 2021), chapter 3, pp. 28-35.

19 Arbuckle and El Emam, Building an Anonymization Pipeline, op. cit., pp. 60-65.

20 Ohm, "Broken Promises of Privacy," op. cit., pp. 1740-1746.

duced<sup>21</sup>. Regional data governance instruments addressing classification questions in Southeast Asia have generally framed the analysis in terms of re-identification risk rather than data format, which suggests this approach is not unfamiliar within the region<sup>22</sup>. The principal difficulty with this approach is evidentiary: it requires a method for assessing re-identification risk that Cambodian law has not yet developed, and that assessment may not always yield a clear answer.

## D. Implications for Cambodia

Cambodian sectoral regulation already demonstrates a preference for obligations calibrated to the sensitivity of information rather than a single uniform rule. The National Bank of Cambodia's directive on credit reporting requires consumer consent before credit information is used for purposes beyond those specifically permitted, and limits retention periods by reference to the type of information involved<sup>23</sup>. This reflects a regulatory instinct, in at least one Cambodian sector, to differentiate obligations by reference to the sensitivity and intended use of information, even though it falls short of an established risk-tiered framework. A standard that classifies synthetic data according to re-identification risk would draw on a similar instinct, applied for the first time to data protection rather than credit information.

Each of the three approaches carries a different cost. Categorical exclusion accepts a risk of under-protection under Article 32 in exchange for administrative simplicity. Categorical inclusion accepts a risk of over-regulation in exchange for removing any incentive to relabel personal information as synthetic. A risk-based approach attempts to track the actual risk to individuals but requires institutional capacity, including technical guidance and a method for assessing evidence, that does not yet exist in Cambodia. Whichever direction Cambodian regulators take, the choice should be made deliberately, with reference to which of these costs Cambodia is better positioned to manage, rather than left unresolved by omission.

## V. Conclusion

Cambodia's existing instruments, built around directly collected or directly held information, do not supply a rule for classifying data generated by a computational model trained on real records. This is not a minor gap. It leaves open basic questions of accountability when synthetic data is shared or transferred, of responsibility when re-identification causes harm, and of predictability for organizations attempting to comply with Article 32 in good faith. Of the three approaches considered, categorical exclusion and categorical inclusion each resolve the uncertainty at the cost of disregarding a factor the other treats as central: actual identifiability risk, in the case of exclusion, and proportionality to that risk, in the case of inclusion. A risk-based approach engages directly with the question that distinguishes one synthetic dataset from another, namely whether the individuals behind it remain reasonably identifiable. However, it requires institutional tools that Cambodia has not yet built. As synthetic data becomes more widely used across Cambodia's banking, healthcare, and technology sectors, the cost of leaving this question unresolved is likely to grow rather than diminish. Whatever approach is eventually adopted, Cambodian law would benefit from addressing the classification of synthetic data explicitly under Article 32, rather than allowing the question to be answered by default through silence.

<sup>21</sup> Law on Electronic Commerce, op. cit., art. 32.1; see also Schwartz and Solove, "The PII Problem," op. cit., pp. 1820-1825.

<sup>22</sup> ASEAN Secretariat, ASEAN Data Management Framework, op. cit., chapter 3, pp. 28-35.

<sup>23</sup> National Bank of Cambodia, Prakas on Credit Reporting, B7-018-243 (2018); see also Jay Cohen and Chandavya Ing, "Cambodia," in *Cybersecurity and Data Protection in Mainland Southeast Asia* (Tilleke & Gibbins, 2024), <https://www.tilleke.com/wp-content/uploads/2024/07/Tilleke-Cybersecurity-and-Data-Protection-in-Mainland-Southeast-Asia-2024.pdf>, p. 4.

## Bibliography

### Legislations

1. Kingdom of Cambodia. Civil Code. 2007.
2. Kingdom of Cambodia. Constitution of the Kingdom of Cambodia. 1993, as amended.
3. Kingdom of Cambodia. Law on Electronic Commerce, Royal Kram No. NS/RKM/1119/017. 2019.
4. Kingdom of Cambodia. Law on Telecommunications, Royal Kram No. NS/RKM/1215/017. 2015.
5. Kingdom of Cambodia. National Bank of Cambodia. Prakas on Credit Reporting, B7-018-243. 2018.

### Books

1. Arbuckle, Luk, and Khaled El Emam. Building an Anonymization Pipeline: Creating Safe Data. Sebastopol: O'Reilly Media, 2020.

### Journal Articles

1. Carlini, Nicholas, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Tramer. "Membership Inference Attacks From First Principles." 2022 IEEE Symposium on Security and Privacy: pp. 1897-1914.
2. Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review 57 (2010): pp. 1701-1777.
3. Schwartz, Paul, and Daniel Solove. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." New York University Law Review 86, no. 6 (2011): pp. 1814-1894.
4. Stadler, Theresa, Bristena Oprisanu, and Carmela Troncoso. "Synthetic Data -- Anonymisation Groundhog Day." Proceedings of the 31st USENIX Security Symposium (2022): pp. 1451-1467. <https://www.usenix.org/conference/usenixsecurity22/presentation/stadler>.

### Reports and Policy Documents

1. ASEAN Secretariat. ASEAN Data Management Framework. Jakarta: ASEAN, 2021.
2. Cohen, Jay, and Chandavya Ing. "Cambodia." In Cybersecurity and Data Protection in Mainland Southeast Asia. Tilleke & Gibbins, 2024. <https://www.tilleke.com/wp-content/uploads/2024/07/Tilleke-Cybersecurity-and-Data-Protection-in-Mainland-Southeast-Asia-2024.pdf>.
3. Cambodian Center for Human Rights / LICADHO. "Cambodia's Law on Telecommunications: A Legal Analysis." Phnom Penh, March 2016. [https://www.licadho-cambodia.org/reports/files/214LICADHO-TelecomsLawLegalAnalysis\\_March2016ENG.pdf](https://www.licadho-cambodia.org/reports/files/214LICADHO-TelecomsLawLegalAnalysis_March2016ENG.pdf).



#### 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  
Email : [Office.PhnomPenh@kas.de](mailto:Office.PhnomPenh@kas.de)  
Website : [www.kas.de/cambodia](http://www.kas.de/cambodia)  
Facebook : [www.facebook.com/kaskambodscha](https://www.facebook.com/kaskambodscha)