KONRAD ADENAUER STIFTUNG

LAW BRIEF 2.0
DIGITAL LAW

ABOUT LAW BRIEF

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

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

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

ABOUT KAS FOR LEGAL YOUTH (KASFLY)

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

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

Production Editors
PAUL MORNET
SEREIVATHNA BUNNY

Proofreading By
MAKLIKA LENG
NEJRA LILIC

Layout Design
VIRAK DUONG

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.

ABOUT KONRAD-ADENAUER STIFTUNG

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

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

Learn more through KAS Cambodia Website.

ABOUT ROYAL UNIVERSITY OF LAW AND ECONOMICS

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

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

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

Editor Note

Cambodia's surging digitalization of its financial sector, consumption patterns and to a lesser extent public services has been accompanied by a multiplication of recently promulgated and upcoming legislative initiatives aimed at modernizing a dated, sporadic and often inconsistent legal framework, especially in the face of the manifold risks and threats brought by these new circumstances. Nevertheless, it appears complex to effectively ascertain the substantive changes brought by these provisions in this context of rapid transformation. This publication is a humble contribution to interpreting some of these changes, with a view to inform public discussions, under four categories: data protection law; digital rights; digital law and fintech; cybercrime and cybersecurity law. It is the product of a six month-long KAS fellowship program comprising of training sessions, study trips and an overall unforgivable journey of friendships and hardships.

It is advised for the reader of this publication to take into consideration a few preliminary remarks before to reach for the collection of briefs. First, the publication is a heterogeneous collection of law briefs which targets various, albeit specific, legal areas of enquiry under the umbrella term 'digital law'. The authors were provided with the academic freedom to identify both the nature and scope of the subject matter under scrutiny. Hence, the publication is to be understood as a horizontal collection of briefs rather than a unified and harmonious demonstration. Second, the publication's heterogeneity is also to be attributed to the decision made to publish all the briefs in their entirety, with little filter applied beyond the formal requirements, resulting in qualitative disparities among the contributions. Third, readers will notice an extensive mobilization of comparative analytical tools in the briefs. This is explained in large parts by the need to make up for the relative absence of doctrine on the subject matter in Cambodia and the difficult access to judicial decisions, but also because foreign instruments in digital law are often perceived as benchmarks for the Cambodian lawmakers resulting in various incoming legal transplants. Given these circumstances, fellows were thus actively encouraged to resort to comparative analysis, which transpires from the publication. Finally, it is essential to keep in mind that all the authors are under-graduate law students and that this publication constitutes their first attempt at the exercise.

My view as editor is that most fellows have demonstrated capacity to move beyond the descriptive habits generally found at this stage of academic development toward embracing analysis, a perilous and demanding journey. Nevertheless, please note that your constructive criticism and enquiries are sought to initiate debates on such important topics and nurture the academic excellence of Cambodia's legal youth.

I wish you a pleasant reading.

PAUL MORNET

Program Director

RULE Dual Degree Department in Law

Contents

Abbreviations

AML/CFT: Anti-Money Laundering and Combating the Financing of Terrorism

CASPs: Crypto-Asset Service Providers

CDD: Customer Due Diligence

DLT: Distributed Ledger Tech

EU: European Union

FATF: Financial Action Task Force

FSA: Financial Services Agency of Japan

Fintech: Financial Technology

GDPR: General Data Protection Rights

IoT: Internet of things

Japan's PSA: Japan's Payment Services Act

MAS: Monetary Authority of Singapore

MEF: Ministry of Economy and Finance

MiCA: EU's Markets in Crypto-assets and Amending Regulations

MPTC: Ministry of Post and Telecommunication

NBC: National Bank of Cambodia

NBFSA: Non-Bank Financial Services Authority

RGC: Royal Government of Cambodia

SERC: Securities and Exchange Regulator of Cambodia

Singapore's PSA: Singapore's Payment Services Act

Section 1
Data Protection Law

Source: Forage

INTERPRETING THE AMBIGUITIES OF THE TERMS UNDER ARTICLE 32 OF CAMBODIAN LAW ON ELECTRONIC COMMERCE

ENG Sochetra

is a junior double-degree student, majoring in Bachelor of Law, and English Language-Based Bachelor of Law program at Royal University of Law and Economics. He participated in the 31st Willem C. Vis International Commercial Arbitration Moot, responsible for preparing memorials for his university. Currently, he is working as a lawyer assistant at a law firm majorly handling litigation cases. He has strong interests in commercial law and digital law. He is looking forward to contributing in the development of the Cambodian legal framework adapting to the evolving digital field.

I. INTRODUCTION

In the digital era, given the rise of businesses along with the advancement of technologies, the majority of people remain unaware of their personal information being exposed to cyber threats. In 2024, the remarkable increase in data breaches which data compromise amounts to 26 Million, stemming from 3876 incidents in various sectors.[1] These reports underscore the urgent need for robust legal frameworks on data protection to combat cyber threats.

In the Cambodian context, as the government's Digital Economy and Society Policy prioritizes cybersecurity and digital sectors, both the Law on Data Protection and Cybersecurity are in the drafting process.[2] Nonetheless, Cambodian Law on E-commerce expressly provides for E-commerce business operators' obligation to protect their consumers' data. According to Article 32 of Cambodian Law on E-commerce, "any person storing electronic record of private information shall use all means to ensure that the information is reasonably and safely protected."[3] A research paper concerning this provision highlighted some potential issues related to the interpretation of the terms contained therein, such as 'personal information' as well as 'reasonable data protection measures'.[4]

Due to the absence of specific laws addressing data protection matters, how should the data protection provision under Article 32 of the Law on E-commerce be interpreted and implemented?

As of 2024, more than 80 countries and some international organizations have recognized GDPR as a gold standard for data protection compliance regulations, while some countries have taken GDPR as a jumping-off point.[5] Thus, this law brief aims to provide insights and contributions on how to interpret and implement Article 32 of the Law on E-commerce by stating the need for a clear definition of the term 'private information' [II], a practical approach toward reasonable data protection measures [III], and undue burden toward E-commerce service providers [IV], under GDPR approaches.

II. THE NEED FOR A CLEAR DEFINITION OF THE TERM 'PRIVATE INFORMATION'

Due to the absence of specific law, none of the existing interpretations of the term 'personal data' depend on relevant laws. Nonetheless, under Cambodian E-commerce Law, the term 'data' is defined as "a group of numbers, characters, symbols, message, images, sound, video, information or electronic program which are prepared in a form suitable for use in a database or an electronic system."[6] By this definition, the 'data' not only consists of the information stored digitally but also of various contents contained in its definition. With regards to the provision title, it is written as "data protection".[7] However, the first paragraph under this provision expressly only states "private information storing in electronic forms" that is subject to be protected from any wrongful acts. In this regard, Article 32 (1) states only 'private information that is electronically stored', which, in contrast to its title, would leave a large gap for relevant actors to exploit this provision when it comes to interpreting and implementing such provision.

As of 2024, a sub-decree was adopted, introducing two terms related to personal data.[8] First, "personally identifiable data" refers to any information which is capable of identifying a person.[9] Second, "personal information" refers to a combination of data that is capable of learning the information related to private

[1] Kyna Kosling, "Global Data Breaches and Cyber Attacks in January 2024 – 29,530,829,012 Records Breached," IT Governance UK Blog, February 5, 2024, https://www.itgovernance.co.uk/blog/.
[2] "EuroCham: Cambodia Continues Development of Data Protection Laws, Experts Highlight Importance of Aligning With ASEAN Standards - Cambodia Investment Review," February 5, 2024, https://cambodiainvestmentreview.com/2024/02/05/eurocham-cambodia-continues-development-of-data-protection-laws-experts-highlight-importance-of-aligning-with-asean-standards/ .
[3] Law on Electronic Commerce, No. NS/RKM?1119/017, November 2 2019, Article 32 (1).
[4] Phin Sovath, "Privacy and Data Protection in the Digital Age: A Holistic Approach to Privacy and Data Protection in Cambodia," in Law in the Digital Age: Protection of Consumer Rights, eds. Kong Phallack, Long Chanbormey (2021), p. 67.
[5] Sears, Emilie. "International Regulations and the GDPR-Effect." RadarFirst, October 12, 2021. https://www.radarfirst.com/blog/international-regulations-gdpr-effect/.
[6] Law on Electronic Commerce, No. NS/RKM?1119/017, November 2 2019, Annex, Definition
[7] Law on Electronic Commerce, No. NS/RKM?1119/017, November 2 2019, Article 32 (1).
[8] Sub-Decree on the Management, Use, and Protection of Personally Identifiable Data, No. 252 អនក្រ.បក dated 22 December 2021
[9] Sub-Decree on the Management, Use, and Protection of Personally Identifiable Data, No. 252 អនក្រ.បក dated 22 December 2021, Article 3.

living or confidentiality of a person.[10] Similarly to the provision under GDPR, the term "personal data" refers to "any information relating to an identified or identifiable natural person."[11] Comparing the term "personally identifiable data" provided under the sub-decree, GDPR provided a broader exhaustive list referencing some identifiers.[12] As for information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation are considered as sensitive data, and subject to categorizing separately and different regulation of use and processing.[13] This information may constitute "personal information" in the Cambodian context, provided it relates to individuals' private lives and confidentiality. Regarding confidential information, the concept of protecting this information has been addressed through sectoral laws, including labor,[14] banking,[15] insurance.[16]

Given the broad conception of "personal data" used in GDPR, such enormous scope of application may also lead to challenges in terms of actual compliance and enforcement.[17] Although the terms "personally identifiable data" and "personal information" may already be defined. The scope of its application remains limited. Moreover, the definition seems to be broadly defined. Regarding Article 32 of the Law on E-commerce, the unclear definition of "private information stored in digital form" seems to limit its scope of protection. Thus, a clear definition of "personal data" should be defined under the Law on E-commerce to determine the scope of data protection, not just limited to "private information storing in digital form". Apart from this, as not all types of information are considered as confidential, the classification of such data should also be taken into consideration, provided some specific types of data in diverse sectors may be subject to different regulations.

III. PRACTICAL APPROACH TOWARD REASONABLE DATA PROTECTION MEASURES

Despite lacking comprehensive laws addressing requirements for reasonable data security measures, the Law on E-Commerce still deliberately mandates businesses to secure their consumers' data without providing the requirements or specific criteria to be considered when implementing the security measures. While diverse sectors may require different considerations, the cyber security framework practice implemented by the National Bank of Cambodia ("NBC") could be a reference point, provided it is the only existing cyber security framework amongst other sectors. In 2019, in response to the rise of cyber financial fraud, the NBC adopted a guideline to enhance the safety, security, and efficiency of business operations, ranging from IT governance to information security audits.[18] It further addressed some guidance on data security, offering extensive criteria for mitigating the risks and ensuring their security system.

Due to the absence of comprehensive regulations addressing these issues, the existing cyber security standards could help interpret the "reasonableness of the security measures" under Article 32 of the Law on E-commerce. In 2021, Cambodia adopted an "ISO/IEC27001" which serves as a standard framework for managing information security.[19] It provides guidelines for establishing formalized information security management systems ("ISMS") within the context of the organization's overall business risks to fit the

[10] Ibid.
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, referred as "GDPR") Article 4 (1).
[12] Ibid.
[13] Vrabec, Helena U. Data Subject Rights under the GDPR. 1st ed. Oxford University Press Oxford, 2021. https://doi.org/10.1093/oso/9780198868422.001.0001.
[14] Cambodian Labor Law, No. CS/RKM/0397/01, March 13 1997, Article 239.
[15] Law on Negotiable Instruments, No. NS/RKM/1005/030, Article 221 (1).
[16] Law on Insurance, No. NS/RKM/0814/021, August 4 2014, Article 106.
[17] Kuner, Christopher, Lee A. Bygrave, and Christopher Docksey, eds. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, United Kingdom: Oxford University Press, 2019, p. 113.
[18] National Bank of Cambodia, Technology Risk Management Guidelines, (2019), p.5.
[19] SecuDemy.com. "កម្ពុជាដាក់ឱ្យប្រើប្រាស់ស្តង់ដារនីតិវិធីគ្រប់គ្រងសន្តិសុខសាយប័រ." Retrieved. https://secudemy.com/cambodia-cybersecurity-standards/.

needs of individual organizations or parts thereof, regardless of type, size, and nature.[20] This set of controls for the control and mitigation of the risks associated with the information assets that the organization seeks to protect by operating its ISMS.[21]

In considering the reasonableness of the data security measures, GDPR listed four types of security measures, which are the pseudonymization and encryption of personal data; the ensuring of ongoing confidentiality, integrity, availability, and resilience of processing systems; the ability to restore the availability and access to personal data in a timely manner; and a process for regularly testing, assessing, and evaluating the effectiveness of security measures.[22] These requirements align with the framework adopted by NBC in terms of mitigating unforeseeable risks as well as maintaining critical cyber infrastructure. Moreover, in the practice of GDPR reasonable security measures compliance, the ISO27001 information framework as well as the NIST security framework have been internationally recognized for implementing their risk-based approach.[23]

Implementing ISO/IEC27001 should be interpreted as an essential requirement in considering the reasonableness of the data protection measures under Article 32 of the Law on E-commerce. As the existing standard does not have the legal effect of binding any relevant actors,[24] a comprehensive law addressing specific security measures in accordance with international practice is strongly needed.

IV. UNDUE BURDENS TOWARD E-COMMERCE BUSINESS OPERATORS

As Article 32 of the Law on E-Commerce expressly states, "all persons" have an obligation to use all means in securing their personal information.[25] Such provision may impose excessive burdens on businesses, provided the terms "all persons" may include both natural and legal persons under the Cambodian Civil Code. Such interpretation opens the door to putting excessive burdens on either the natural person or the legal person in terms of complying with laws due to the low financial resources and lack of practical experience in the cybersecurity field. Regarding the data security obligation, Article 32 of the GDPR broadens the data security obligations by obliging both data controllers and the data processor to implement appropriate measures in securing the data of the individuals.[26] The data controller could either be a natural or legal person who determines the purposes and means of the processing of personal data.[27] Whereas a data processor refers to an entity that processes data for the data controller upon the instruction of the data controller.[28] As these two actors have distinct obligations, their responsibilities would also be varied accordingly in the event of a breach. This approach also aims to ensure and enhance the level of data security as these actors play vital roles in data processing.[29] As the data security obligations may extend to the people acting under the instructions given by the data controllers or processors, GDPR tends to be broad in terms of its application, ranging from the data controllers to any persons in contractual relation with it.[30]

Although GDPR is well-recognized in terms of its data privacy regulations standard, the majority of its innovations, such as security breach notification and monetary fines by wealth-based approach,

[20] ISO/IEC27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, third edition, Swtitzerland: ISO copyright office, (2022), p. 19.
[21] Ibid, p. 20.
[22] Kuner, Christopher, Lee A. Bygrave, and Christopher Docksey, eds. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, United Kingdom: Oxford University Press, 2019, p. 636.
[23] Denley, Andrew, Mark Foulsham, and Brian Hitchen. GDPR – How to Achieve and Maintain Compliance. 1st ed. Routledge, 2019. https://doi.org/10.4324/9780429449970. p. 47.
[24] Law on the Amendment of Cambodian Standard Law, No. NS/RKM/0618/011, June 26 2018, Article 3 (New).
[25] Law on Electronic Commerce, No. NS/RKM?1119/017, November 2 2019, Article 32 (1).
[26] GDPR, Article 32 (1).
[27] GDPR, Article 4 (7).
[28] Kuner, Christopher, Lee A. Bygrave, and Christopher Docksey, eds. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, United Kingdom: Oxford University Press, 2019. p. 160.
[29] Kuner, Christopher, Lee A. Bygrave, and Christopher Docksey, eds. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford, United Kingdom: Oxford University Press, 2019. p. 634.
[30] Ibid. p. 635.

originated in the United States.[31] For instance, the California Consumer Privacy Act ("CCPA") was enacted into law following the GDPR concept, specifically, the right to sue or fine the non-compliant organization.[32] Under its provisions, consumers are entitled to initiate a lawsuit against the business for failing to implement and maintain reasonable security procedures in protecting their personal information.[33] Unlike Cambodian E-commerce Law that refers to "all persons" without specifying the kind of persons, the CCPA specifically uses the term "business", which is defined as a legal entity established to earn annual revenue for a specific amount.[34] In this regard, rather than generally oblige any person who holds the data bearing such obligations, the CCPA binds the business operators, bearing direct connection with the consumers.

In this regard, different actors have distinct obligations, and their liabilities may also be diverse if they fail to comply with the law. Therefore, subsequent legal regulations or guidelines on the application of the laws should consider the matters regarding a clear definition and classification of each relevant actor to accord with its specific obligations to establish a clear line of accountability.

V. CONCLUSION

To conclude, this brief intends to discover potential issues regarding the current provision. A single provision under the Law on E-commerce concerning the data security obligation alone would not suffice to deal with the issues related to data security compliance and ensure the highest possible safety of the consumers' data. Despite the lack of such laws, the ambiguities of the terms contained within the provision, such as the persons bearing the data security obligation as well as the reasonableness consideration, not only would make the provision itself impossible to comply with, there would also be various legal conflicts and enforcements in the field of E-commerce in the rise of cyber threats as well as the data breaches. In addition, with the given limited period and sources. It is undeniable that apart from the issues brought up in this research, there are still various issues in this topic, for instance, the concept of consent or the issues related to data security in the context of cross-border transfer, which were not addressed, as well as some other external sources such as the existing laws in various countries and its rationale behind. Last but not least, given Cambodia is still drafting the data-related laws, more comprehensive research of obliging the relevant actors in implementing the data security measures by taking into consideration Cambodia's society, culture as well as its people's economic conditions is highly and critically demanded in establishing an independent law addressing the data protection.

[31] Michael L. Rustad and Thomas H. Koenig, TowardsaGlobalDataPrivacyStandard, 71 Fla. L. Rev. 365 (). Available at: https://scholarship.law.ufl.edu/flr/vol71/iss2/3 p. 443.
[32] Ibid. p. 403.
[33] California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST). § 1798.150.
[34] California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST). § 1798.140.

Law Talk 2022

ENFORCING CLICK-WRAP AGREEMENTS WITHIN THE CAMBODIAN LEGAL SYSTEM: CHALLENGES AND SOLUTIONS

SENG Mathyna

is an assistant at the Phnom Penh Court of First Instance, where she applies her theoretical legal knowledge into practice. She is a fourth-year student pursuing dual law degrees, a Bachelor of Law and an English-Language Based Bachelor of Law, at the Royal University of Law and Economics, supported by a Raoul Wallenberg Institute scholarship. She has also engaged in moot court competitions, both as a participant and an advisor, including the International Humanitarian Law (IHL) and Nuremberg Moot Court Competitions. In addition to her studies, she has served as an officer in youth organizations such as AIESEC and the university student community. She is also a KASFLY Fellow 2024, and her research interests are in Digital Law, Criminal Law, and E-commerce Law.

I. INTRODUCTION

Electronic contracts form the basis of agreements in E-commerce. According to Article 12 of the Law on E-commerce, offers, acceptances, and contracts can be conducted electronically. Such contracts are considered valid, legally effective, and enforceable when the offer and acceptance align, even when completed through electronic means.[1] The United Nations Commission on International Trade Law Model Law on Electronic Commerce with Guide to Enactment also stated that an offer and the acceptance of an offer may be expressed using data messages, meaning it shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose,[2] signifying that contracts made electronically are accepted internationally.

One common type of agreement encountered while browsing the internet is the "Click-wrap agreement." This type of agreement involves individuals reviewing the terms and conditions presented on a website and expressing their consent by clicking "I AGREE" or "I DISAGREE." Another type of click-wrap agreement prevalent in everyday internet use is the agreement to accept or deny 'cookies.' These agreements are prevalent when downloading, selling, viewing, or buying products or services online. It is important to highlight that artificial intelligence in current development does not possess the capacity to establish legally enforceable contracts. Thus, if Siri, an artificial intelligence virtual assistant, for example, provides information through voice control, it cannot give assent or dissent to any terms, making it incapable of concluding valid contracts.[3] As a legal person, you have the responsibility to decide whether to provide your information. The absence of safety standards for the type of information transferred and exchanged through the grey area of online agreements, such as click-wrap agreements, emphasizes the need to thoroughly assess Cambodia's current legislation on e-commerce and consumer protection. This scrutiny is essential to prevent detrimental consequences for citizens to avoid data violation incidents.

As such, to analyze the grey area of click-wrap agreements in Cambodia and possible solutions to avoid data violation and more, it is crucial we navigate the legal maze in understanding click-wrap agreements by understanding the loophole that exists in Cambodia's current legislation such as Law on E-commerce and Law on Consumer Protection, assess the legal problem of implementing the Click-Wrap Agreement in Cambodia, possible remedies and recommendation that can be compensated to individuals of those violations.

II. NAVIGATING THE LEGAL MAZE: CHALLENGES IN CLICK WRAP AGREEMENT

1. THE DIGITAL LOOPHOLE FOUND IN CAMBODIA'S LEGAL FRAMEWORK

A. LAW ON ELECTRONIC COMMERCE

Under the Law on E-commerce in Cambodia, information standards have been given for digital consumer protection.[4] Article 32 of the Law on Electronic Commerce mentions that any person who holds personal information in electronic form shall use all means to ensure that the information is protected from loss or being disclosed;· Still, this provision does not specify which person's character can hold the information legally. Moreover, the standard of safety protection of private information is not defined,[5] if consumer data are held freely by a data controller and data processor,[6] with the only obligation of using "all means" possible as a form of protection against leakage of such data, highlights a significant loophole in ensuring adequate online consumer protection in Cambodia's electronic commerce. Furthermore, as mentioned in the article, the party must take all measures under all reasonable circumstances, but the article does not elaborate on what "all measures" means or what a "reasonable circumstance" refers to.[7] Hence, there

[1] Law on Electronic Commerce, Article 12.
[2] Model Law on Electronic Commerce with Guide to Enactment 1996: With Additional Article 5 Bis as Adopted in 1998, Article 11.
[3] Huzefa Tavawalla & Abhishek Senthilnathan, "Can Artificial Intelligence be given Legal Rights and Duties?", Business Standard, June 19th, 2018, page 1.
[4] Tilleke & Gibbins, "What Cambodia's New Law on Electronic Commerce Means for Business", 2020, page 16.
[5] Tilleke & Gibbins, "Responding to a Data Breach in Southeast Asia", August 2023, page 5.
[6] Jay Cohen, Sochanmalisphoung Vannavuth, Chandavya Ing (Tilleke & Gibbins International Ltd.), Cambodia - Data Protection Overview, October 2023. (Accessed 25 April 2024) https://www.dataguidance.com/notes/cambodia-data-protection-overview
[7] Keo Sothie, "Cambodia's Culture and Laws on Privacy and Data Protection, and the Future", Law in the Digital Age: Protection of Consumer Rights, (Konrad Adenauer Stiftung: November 2021), Page 47.

is a clear imperative to enhance enforcement regarding the obligations of individuals holding personal information. It is crucial to specify the precise scope of measures required to protect consumers in Cambodia adequately.

B. LAW ON CONSUMER PROTECTION

Moreover, the provisions under the Law on Consumer Protection in Cambodia are related to consumer rights, product safety standards, advertising regulations, unfair contract terms, and mechanisms for dispute resolution.[8] In addition, any person using electronic communications for commercial activities with consumers shall comply with all other provisions and regulations related to consumer protection.[9]

Furthermore, this legislation addresses the standard of information required to be provided to customers for businesses to comply with.[10] However, it does not regulate the handling of consumer information such as age, name, nationality, or other personal details.[11] This demonstrates the extension of consumer protection scope to online markets. However, these regulations presently lack enforceable penalties and comprehensible paths in pursuing remedies for the personal data of individuals negatively impacted by online market transactions and e-agreements. Consequently, there is a crucial need for legislative enhancement to establish robust safeguards for citizens against online consumer violations.

2. ASSESSING THE LEGAL ISSUE OF IMPLEMENTING CLICK WRAP AGREEMENT IN CAMBODIA

A. EVALUATING THE SECURITY OF CLICK WRAP AGREEMENTS: FRAUDULENT INTENT

In order to combat fraudulent cases in e-commerce transactions, provisions have outlined that a person who uses electronic communications to sell goods or services to consumers shall provide accurate, clear, and easy-to-understand information on the goods and services.[12] In a commercial transaction, the essential terms and conditions that must be disclosed are payment method, withdrawal or cancellation of an order, termination, delivery, and exchange of goods and refund.[13] However, regarding other agreements such as click-wrap agreements, the terms and conditions, or cookies,[14] are not specifically regulated, such as regulation over the consent of their data after accepting cookies, data retention, and more.

Moreover, an individual, upon interaction with click-wrap agreements on an e-commerce website or similar online platform, may lack awareness of the terms governing their relationship with the respective company or website owner.[15] Consequently, said individual may unintentionally provide consent to specific uses of their personal information, which they may not endorse.[16] If companies decide to sell or unlawfully exploit such data obtained from consumers, individuals have limited means to safeguard themselves from potential risks, including the unauthorized distribution of their disclosed data or its correlation with information from diverse sources, leading to the profiling of users by various entities and organizations.[17] If these cookies agreements are left unregulated, it paves the way for potential future breaches regarding cookies, akin to the Commission Nationale Informatique & Libertés's case where Amazon Europe Core was fined €35 million ($38 million) for deploying advertising cookies on users'

[8] Law on Consumer Protection, Article 1.
[9] Law on Electronic Commerce, Article 33.
[10] Law on Consumer Protection, Article 27.
[11] Phin Sovath, "Privacy and Data Protection in the Digital Age: A Holistic Approach to Privacy and Data Protection in Cambodia", Law in the Digital Age: Protection of Consumer Rights, November 2021, page 57.
[12] Law on E-commerce, Article 29.
[13] Law on e-commerce, Article 29; Prakas on Information Standard on Customer, Article 9.
[14] Cloudflare, "What Are Cookies?", (Accessed March 23, 2024). https://www.cloudflare.com/learning/privacy/what-are-cookies/ Cookies are a type of data created by an internet server while browsing a website that is sent to a web browser.
[15] Nili Steinfeld, "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment, in Computers in Human Behavior, Volume 55, Part B, (February 2016), page 6.
[16] Ibid.
[17] Ibid.

computers without consent or adequate disclosure on the Amazon.fr sales site.[18] Therefore, the absence of regulation poses a threat to citizens accessing websites employing click-wrap agreements.

B. UNDERSTANDING CLICK-CONSENT: A PERMANENT COMMITMENT?

Online terms and conditions are legally binding, given in situations where consumers on the internet have given consent, such as by clicking an "I AGREE" button or entering their name into a signature box, thus signifying consent.[19] However, for consumers, it's like navigating a maze: not only do they wonder what happens to their data after clicking "agree", but they also struggle to grasp and influence the kinds of data gathered online.[20] Understanding the technicality and legal issues in the form of a simple click-and-agree mechanism required training and sufficient information.[21] Generally, a click-consent is implied to be a form of 'forever-consent',[22] thus raising issues in situations such as the terms and conditions of the data processor have changed, but the implied consent stays the same.[23]

In addition, in a situation where the use and disclosure of the personal data is for a purpose different from which it was initially collected, the service provider using the data would need to notify the individual,[24] of the new purpose and obtain new consent unless:

"a. the new purpose is within the scope of the original consent; or

b. where implied consent can be established.

c. implied consent refers to any act generally recognized as consent under applicable trade practices. However, express and written consent should be obtained if the service provider wishes to use or disclose personal data for a purpose different from the one for which it was collected.

d. when a service provider is seeking consent from the data subject, the service provider must disclose or notify the data subject of the purpose(s) for which it intends to collect, use, or disclose the data subject's data before such collection, use or disclosure of the personal data."[25]

However, Cambodian laws do not prescribe a way for an organization to notify individuals of such change, [26] leaving the choices of the notification up to the organization. [27] Furthermore, disclosures/notifications to the individuals regarding the purpose of the collection, use, and disclosure of personal data must not be too vague or broad in scope so that the consumer can easily understand the direction their data are going and being collected for what purposes.[28]

C. DATA BREACH: UNRAVELLING THE VIOLATION

Click-wrap agreements are the technicality behind cookies, which allow the browser to store information in a text file and then send it back to the server each time the browser accesses it. The primary function of a cookie is to help the server recognize the browser. Online Websites will then utilize all of the cookies

[18] Commission Nationale Informatique & Libertés, Cookies: the Council of State confirms the 2020 sanction imposed by the CNIL against Amazon, 28 June 2022. (Accessed on 24 May 2024) https://www.cnil.fr/en/cookies-council-state-confirms-2020-sanction-imposed-cnil-against-amazon; Cookieyes, 8 Companies Hit with Cookie Consent Fines for Non-Compliance, May 13th, 2024. (Accessed on 24 May 2024) Available in: https://www.cookieyes.com/blog/cookie-consent-fines/.
[19] Joao Vitor Sales, "Are Terms and Conditions Legally Binding?" Website Policies, August 1, 2023. (Accessed March 22, 2024) https://www.websitepolicies.com/blog/are-terms-and-conditions-legally-binding.
[20] Natali Helberger et al., "Consent and post-consent data management in EU data and consumer protection law", in EU CONSUMER PROTECTION 2.0: Structural asymmetries in digital consumer markets (Brussels, March 2021), page 32.
[21] Ibid.
[22] Bart Custers, "Click here to consent forever: Expiry dates for Informed Consent", Big Data & Society, January–June 2016, page 1. https://doi.org/10.1177/2053951715624935.
[23] Ibid.
[24] Jay Cohen, Sochanmalisphoung Vannavuth, Chandavya Ing (Tilleke & Gibbins International Ltd.), Cambodia - Data Protection Overview, October 2023. (Accessed 25 April 2024) https://www.dataguidance.com/notes/cambodia-data-protection-overview.
[25] Ibid.
[26] Tilleke & Gibbins, "Responding to a Data Breach in Southeast Asia", August 2023, page 2.
[27] Jay Cohen, Sochanmalisphoung Vannavuth, Chandavya Ing (Tilleke & Gibbins International Ltd.), "Cambodia - Data Protection Overview", October 2023. (Accessed 25 April 2024) https://www.dataguidance.com/notes/cambodia-data-protection-overview.
[28] Natali Helberger et al., "Consent and post-consent data management in EU data and consumer protection law", in EU CONSUMER PROTECTION 2.0: Structural asymmetries in digital consumer markets (Brussels, March 2021), page 37.

collected to identify and track users, update user preferences, and save previously entered information, such as names, addresses, or passwords.[29]

A breach of internet privacy, a violation of data, can be defined as unauthorized access to any sort of information using information systems available.[30] According to Anderson A. L. Queiroz, an internet breach of privacy can happen when a hacker can obtain access to a victim's account through a malicious maintenance link sent to the victim. In such a situation, when the website is being maintained, cookies that have been input on a website before can be used maliciously later.[31] Due to the absence of regulation on data breach protocol and regulators in Cambodia,[32] it is imperative to regulate the exchange of cookies and data windows to avert such violations.

III. BRIDGING GAPS: RECOMMENDATIONS AND REMEDIES FOR DATA PROTECTION IN CAMBODIA

1. PROPOSED SOLUTION ON CAMBODIA's LEGISLATION

A way forward for the Law on E-commerce in Cambodia is to clearly define which entities are legally allowed to access consumer data. Furthermore, the law should establish robust standards for protecting consumers' personal information, requiring a level of protection against data leakage that exceeds "all means". Finally, the scope of "all measures" and what constitutes "reasonable circumstances" for protecting consumer data should also be explicitly and comprehensively defined to ensure robust data protection.

In order to ensure the effective implementation of the Law on Consumer Protection in Cambodia for both online and physical markets, it is necessary to develop additional enforceable penalties specifically addressing violations related to consumer personal data. Establishing penalties for mishandling consumer information, such as age, name, nationality, or other personal details, will help address this issue. By closing this legal gap, significant contributions will be made to safeguard citizens against online consumer violations.

In addressing these issues, the General Data Protection Regulations ("GDPR") can be a prime example to align Cambodia's principles with in establishing a legal framework to protect consumers regarding these issues legally. The GDPR specifies what types of measures must be taken under what kind of circumstances to protect people's data.[33] It also imposes other obligations specifying clear steps to consider for both the consumer and data processor. For instance, Article 82 of GDPR clearly sets the obligation that any controller involved in processing shall be liable for the damage caused by the processing of data.[34] Furthermore, penalties should also be established in order to achieve efficient enforcement of obligations that each data controller needs to adhere to. Such penalties shall be effective, proportionate, and dissuasive.[35] These are among the numerous measures Cambodia must consider when adopting a more comprehensive data protection framework. However, it should be noted that not all of the GDPR's measures should be adopted as Cambodia's culture regarding data privacy is different from that of the European Union.[36] Hence, the adoption and implementation of such regulation about data regulation need to be carefully trodden upon.

[29] Cornell Law School, "Cookies," Legal Information Institute. (Accessed 20 March 2024) https://www.law.cornell.edu/wex/cookie.
[30] Anderson A. L. Queiroz & Ruy J. G. B. de Queiroz, "Breach of Internet Privacy through the use of Cookies", 23 June 2010, page 2. https://doi.org/10.1145/1839294.1839378.
[31] Ibid.
[32] Tilleke & Gibbins, "Responding to a Data Breach in Southeast Asia", August 2023, page 1.
[33] Keo Sothie, "Cambodia's Culture and Laws on Privacy and Data Protection, and the Future", Law in the Digital Age: Protection of Consumer Rights, op. cit., page 48.
[34] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016, Article 82.
[35] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016, Article 84.
[36] Keo Sothie, "Cambodia's Culture and Laws on Privacy and Data Protection, and the Future", Law in the Digital Age: Protection of Consumer Rights, op. cit., Page 48.

2. STRENGTHENING DATA OBLIGATION COMPLIANCE: ESTABLISHING AND ENHANCING PENALTY FRAMEWORKS

Under E-Commerce Laws in Cambodia, violating data protection obligations, such as failure to provide clear and straightforward opt-out instructions for unsolicited marketing communications,[37] will subject the organization to a written warning, suspension, or revocation of business licenses and permits, and/or turning off the means of marketing and communication to individuals.[38]

In addition, violations such as failure to comply with the Consent, Purpose Limitation, Disclosure / Notification, and Protection Obligations will subject the organization to Imprisonment from 1 to 2 years and a fine amounting to KHR 2 million to KHR 4 million (approx. USD 500 to USD 1,000) and failure to comply with the Retention Obligation will subject the organization to Imprisonment from 1 month to 1 year and a fine amounting to KHR 100,000 to KHR 2 million (approx. USD 25 to USD 500).[39]

However, aside from the above penalties, no legislation nor penalties have been made to efficiently relay justice and compensation for consumers whose data and harm have been caused by data disclosure of click-wrap agreements, such as data breach, the retention of consent, and fraudulent intent in click-wrap agreements. Cambodia could align its regulations more closely with the European Union's directive on Consumer Protection liabilities to enhance consumer data protection measures. [40] This involves not only establishing penalties for infringements but also ensuring robust enforcement mechanisms.[41] Penalties should also be crafted to be both practical and dissuasive, proportionate to the severity of the violation.[42] By adopting such principles, Cambodia can strengthen its legal framework and better safeguard consumer privacy in the digital world.

IV. CONCLUSION

The ongoing interpretation of Click-wrap agreements in the field of legislation raises concerns regarding party anonymity, digital violations, and the effectiveness of e-agreements, particularly click-wrap agreements, as well as the efficacy of enacted legislation. Addressing these legal challenges and finding viable solutions is crucial to safeguarding Cambodian citizens from potential violations.

To address these issues, Cambodia can align its fundamental principles with the EU's consumer protection standards to protect consumers' vital online data more effectively. Furthermore, Cambodia can draw from various legislative frameworks and guiding principles, taking into account its cultural approach to privacy, to develop clearer mechanisms and legislation that adapt to the evolving technological landscape. By doing so, Cambodia can establish a more robust legal framework to protect consumer interests in the digital realm.

[37] Law on Electronic Commerce, Article 58.
[38] Law on Electronic Commerce, Article 52.
[39] Law on Electronic Commerce, Chapter 11.
[40] Directive on Consumer Protection, 2011/83/EU, 2011.
[41] Directive on Consumer Protection, 2011/83/EU, 2011, para. 57, page 22.
[42] Ibid.

Source: CG Technology

ENHANCING CORPORATE ACCOUNTABILITY IN THE WAKE OF DATA BREACH IN CAMBODIA'S LEGAL SYSTEM

RITH Sopheakneath
is a junior associate at Mar & Associates, one of the best corporate law firm in Cambodia. She holds two bachelors degrees of law program at Royal University of Law and Economics (English Law program and Khmer Law program). She participated in the 21st Willem C. Vis East International Commercial Arbitration Moot that was held in Hongkong as a mooter. She has a strong interest in Commercial law, dispute resolution, Intellectual Property and M&A.

I. INTRODUCTION

Personal data privacy has become increasingly fragile in today's technological world.[1] As people and entities' digital footprints expand, so does the threat of compromising breaches that loom over individuals and businesses. The rapid growth of Cambodia's digital sector points to legal system shortfalls in efforts to provide personal data protection in the workplace. Reports from DataGuidance by OneTrust[2] and the OHCHR [3] emphasize Cambodia's data protection difficulties, including the lack of comprehensive legislation and worries about coercive monitoring regulations.

There is an urgent need for Cambodia to improve its legal framework on personal data protection. For now, Cambodian businesses pursuing digitalization strategies can fall victim to regulatory lag produced by the lack of legal tools for notification and accountability after a data breach. This legal vacuum can dramatically affect customers' privacy and confidence in the technical systems on which the digital economy increasingly relies. For instance, GDPR imposes strict rules on notification and accountability in case of data breach. A brief look at the international regulatory landscape surveyed in this short article offers interesting principles of transparency and accountability to strengthen Cambodia's answer to data breaches.

Cambodia's current legal status of personal data protection is piecemeal and lacks a unified approach. Constitutional provisions and legislation on E-Commerce, Telecommunications, and the Civil Code deal with personal data. However, their fragmented approach complicates the enforcement of measures and diminishes corporate accountability for data breaches. Moreover, there is still no law to protect data in general and e-commerce in particular, and this is a serious risk to individuals' privacy and the development of the digital economy in Cambodia.[4] The lack of legislative techniques to regulate data privacy and security makes consumers hesitate to invest and do business in digital commerce. Therefore, Cambodia must make legislation covering both aspects to improve the rule of law. Cambodia should consider the following international principles of transparency and accountability when responding to data breaches.[5]

The following article seeks to provide a systematic and coherent approach to tackle the challenges posed by the unpreparedness of Cambodian legislation in the wake of a data breach. It proposes a review and possible adaptation of some GDPR-like principles in the Cambodian context. After a neutral analysis of selected articles of the GDPR on data breach notifications, this short paper compares these provisions with the current legislative framework in Cambodia to enhance companies' accountability. This critical review points to the necessity of specific rules requiring the notification of data breaches and establishing clear rules for the accountability of companies.

II. LEGAL FRAMEWORK

1. CAMBODIA'S CONSTITUTION

Article 40 of the Cambodian Constitution, on individuals' fundamental rights and duties, guarantees the right to privacy and confidentiality in correspondence. Therefore, personal data must be inferred from these provisions, as they forbid any arbitrary or unlawful interference with privacy, home, or correspondence. Although it establishes privacy as a right, the Constitution does not delineate specific protections or remedies for data breaches. It lacks clear directives for preventing, reporting, or responding to personal data exposures, particularly in the digital domain.

[1] United Nations Human Rights Office of the High Commissioner, "Privacy and Data Protection Increasingly Precious Asset in Digital Era, Says UN Expert," https://www.ohchr.org/en/press-releases/2022/10/privacy-and-data-protection-increasingly-precious-asset-digital-era-says-un
[2] DataGuidance by OneTrust, "Privacy and Data Protection Increasingly Precious Asset in Digital Era, Says UN Expert."
[3] Ibid.
[4] World Bank, "Benefiting from the Digital Economy: Cambodia Policy Note," July 2018, https://openknowledge.worldbank.org/entities/publication/63c2efe7-f574-569f-98ca-11c3cbf83208
[5] Council on Foreign Relations, "Reforming the U.S. Approach to Data Protection and Privacy," accessed March 31, 2024, https://www.cfr.org/report/reforming-us-approach-data-protection

2. CAMBODIA CIVIL CODE

In Articles 317 and 318, the Civil Code prohibits the infringement of private communications. These provisions acknowledge that correspondence is inviolable and that private conversations must be kept secret.[6] These Articles could be invoked to prevent any unauthorized interception or surveillance of information communicated by persons alone by these means of communication. However, the Civil Code does not expressly extend its application to data protection in electronic form. Most importantly, these Articles do not have any requirements for notifying and subsequent procedures for data breaches. The Civil Code does not address the obligations of those who collect personal data and the rights of those whose personal data in electronic form are unlawfully breached.

3. THE LAW ON ELECTRONIC COMMERCE

The Law on E-commerce, adopted to ensure electronic transactions, prescribes in Article 25 that holders of information shall take all necessary measures as soon as possible to preserve and delete information concerning prohibited or unlawful activities, and Article 32 mandates that data holders shall implement all necessary measures to prevent the loss or unauthorized acquisition, processing, dissemination, disclosure, alteration, or destruction of personal information recorded in a communication or recording system.[7] The above provisions clearly do not achieve complete protection for personal data as the law lacks clear guidelines for assessing the impact of data breaches. Reporting such breaches to the competent authority or the persons affected is not mandatory. There are no rules for remediation and penalties in case of such data breaches.

4. THE TELECOMMUNICATIONS LAW

Article 65(b) of the Law on Telecommunications protects the privacy of every person by mandating that telecommunications providers must take measures to preserve the confidentiality and security of their subscribers' data.[8] This provision could be implicitly interpreted as an obligation of telecommunication providers to ensure the integrity and confidentiality of the data in their possession. Nevertheless, the law does not clearly provide any guidance on what actions telecommunication companies must take when a data breach occurs. There is no legal requirement to inform users about such breaches or to mitigate and respond to such breaches.

While each of these laws plays a tiny part in data protection and privacy in Cambodia by establishing, at least, minimum rights and acknowledging the necessity to protect personal data, they all share a similar shortcoming: none of them adequately addresses data breaches. Entities possessing personal data or individuals whose data has been breached are not required to report such incidents. This legislative void implies that Cambodia's legal system would greatly benefit from a standalone data protection law that addresses such modern issues.

III. LEGAL IMPLICATIONS

Reputational harm is what companies fear most about data breaches. As public data breaches raise awareness and sensitivity to data privacy among consumers, customer trust in a company decreases, stock prices drop, and businesses stand to lose the most. In fact, the 2022 IBM Security Cost of a Data Breach Report found that 83% of businesses experienced more than one data breach in 2022.[9] The International Monetary Fund, in its 2022 report, said the direct cost of data breaches, including lost business and constricted trade, has more than doubled since 2017, with the worst data breaches costing

[6] Cambodia Civil Code, op. cit.
[7] Law on Electronic Commerce, Arts. 25, 32.
[8] Law on Telecommunications, Art. 65(b).
[9] IBM, "Cost of a Data Breach Report 2022," IBM Security, accessed April 14, 2024, https://www.ibm.com/reports/data-breach-action-guide

$2.5 billion in losses. These figures do not include the cost of indirect losses such as reputational harm, cybersecurity enhancement, and litigation.[10]

The Thales 2022 Consumer Digital Trust Index showed that banks and financial services (42%), health providers (37%), and consumer tech vendors (32%) are the most trusted sectors by consumers to handle their personal data.[11] However, data breaches come with significant financial costs. Fines from regulators, legal fees, and breach mitigation expenses can easily reach the millions. The risk here applies particularly to countries with lax data protection laws and where there is no legal requirement to notify data breaches – which can tempt companies to 'hide' incidents. However, taking such a course of action would expose firms to significant legal and regulatory risks. For example, it could trigger regulatory follow-up actions and severe fines. The European Data Protection Board is proposing fines totaling €1.2 billion against Facebook for failing to comply with data protection and notification rules.[12]

Countries with cybersecurity legislation, like the European Union's GDPR, have stringent requirements for reporting data breaches. These legal frameworks require companies to notify the relevant regulator and, in some cases, customers within a specified time period from the breach detection. But in places where such laws are still developing or, as in the case of Cambodia, the legal framework is yet to progress to this stage, breached companies may not feel they are legally required to disclose breaches; thus, the incentive remains to keep quiet. Banks and other financial institutions are considered part of a country's critical infrastructure because they store sensitive financial data, including customer details and transaction records.[13] Thus, a data breach in this sector can impact not only individual customers but also the financial system at large. Cybersecurity laws often target these critical infrastructures to ensure an appropriate level of protection for this data and to ensure reporting of incidents that compromise it.[14] In Cambodia, companies in general, particularly those in critical infrastructure sectors, operate in a legal void with no data protection or cybersecurity laws to guide them. It could be argued, by extension, that data protection principles might apply. However, this would not solve the question of notification and accountability in the event of a breach. Until such an extension is passed in Cambodia, companies have a strong incentive to ensure that their staff keeps any data breaches silent.

1. EMPOWERING CUSTOMERS THROUGH INCREASED AWARENESS AND RIGHT ENFORCEMENT

A. ENHANCING DATA CONTROLLER RESPONSIBILITY AND RISK MANAGEMENT

Data controllers should be aware of and mitigate risks inherent in the processing activities they oversee. Data breaches and other adverse events in processing operations can cause serious harm to data subjects, including financial and identity damage and other privacy theft, if data controllers are unaware and do not act to mitigate associated risks.

B. GLOBAL LEGAL FRAMEWORKS FOR RISK MITIGATION IN DATA PROCESSING

Most legal systems around the world impose certain duties on the data controller to make sure that the former is and remains aware of the associated risks of the respective data processing activity:[15]

[10] International Monetary Fund (IMF), "Global Financial Stability Report: The Quest for Financial Stability in an Era of Disruptive Technologies," IMF, 2022, https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[11] Thales, "2022 Thales Consumer Digital Trust Index," Thales Group, 2022, https://cpl.thalesgroup.com/about-us/newsroom/consumer-trust-personal-data-protection-is-lacking-press-release

[12] European Data Protection Board, "€1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision," 2023, https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

[13] Perkins Coie, "FTC Announces Data Breach Reporting Obligation Under GLBA Safeguards Rule," accessed April 26, 2024, https://www.perkinscoie.com/en/news-insights/ftc-announces-data-breach-reporting-obligation-under-glba-safeguards-rule.html

[14] Federal Trade Commission, "Gramm-Leach-Bliley Act," accessed April 24, 2024, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[15] General Data Protection Regulation (GDPR) EU (2016).

i. General Data Protection Regulation (GDPR) - European Union:

- Article 32, the controller and the processor shall implement appropriate technical and organizational measures for ensuring that the processing of personal data meets the required level of security, appropriateness, and confidentiality, taking into account the risks associated with the processing and the categories of data to be processed; they shall demonstrate that they have implemented such measures.[16]

- Article 34, the controller and the processor shall implement reasonable steps to ensure that technical and organizational measures are put in place that provide an appropriate level of security, including technical and organizational measures to ensure the confidentiality, integrity, and availability of processing systems and services[17]

ii. California Consumer Privacy Act (CCPA) - United States:

While not as prescriptive as the GDPR, the CCPA under Section 1798.150 permits a consumer to bring a civil action against a business entity if the consumer's nonencrypted, nonredacted personal information that the business entity has disclosed violates this title if the business entity fails to implement and maintain reasonable security procedures and practices.[18] The CCPA grants consumers the right to enforce their rights under the statute and imposes duties on companies to protect personal information from unauthorized use or disclosure. Thus, companies that fail to implement reasonable security procedures and practices and thereby allow unauthorized access to California residents' personal information may face litigation.

iii. Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada:

PIPEDA's Clause 4.7 requires that personal information be protected by reasonable security safeguards in the circumstances, considering the information's sensitivity. Clause 4.7.3 of PIPEDA further requires that the security safeguards protect against loss, theft, unauthorized use, disclosure, copying, or misuse, or will result in the accidental loss or destruction of personal information.[19] PIPEDA is broadly applicable, and its violation and strict compliance regime sets a high standard for the protection of data and increases accountability of entities that collect and possess personal information.

C. EVALUATING GDPR'S COMPREHENSIVE APPROACH TO DATA PROTECTION

The GDPR offers a better, more holistic solution in its integration of Articles 24, 32, and 34.[20] These three articles seek to ensure that data controllers understand the risks involved in processing their data and are given clear obligations to implement measures that mitigate those risks effectively. Article 34, in particular, highlights the transparency and trust issues surrounding data security by requiring that data breaches be communicated to data subjects in certain instances.[21] The GDPR approach requires risk assessment, measures to protect personal data, and communicating the risks associated with data breaches to data subjects. Data controllers are put in the driver's seat, so to speak, to prevent data breaches by fully understanding the risks involved and taking appropriate and effective measures to mitigate them.

2. BRIDGING THE LEGAL GAP WITH MANDATORY BREACH NOTIFICATION LAWS

A. THE CHALLENGE OF BREACH NOTIFICATION EFFICIENCY AND EFFECTIVENESS

Data breach notification is thus a significant challenge for data security. After the data breach, notification of the breach to both the regulatory authority and the customers is mandatory as it helps take preventive actions against the breach. Therefore, crafting a legal framework that puts enough pressure on entities to

[16] Ibid., Art. 32.
[17] Ibid., Art. 34.
[18] California Consumer Privacy Act (CCPA), Sec. 1798.150.
[19] Personal Information Protection and Electronic Documents Act (PIPEDA), Clauses 4.7, 4.7.3.
[20] General Data Protection Regulation (GDPR), Arts. 24, 32, 34.
[21] Ibid., Art. 34.

disclose data breaches promptly and, at the same time, ensure that the disclosed data is responsible and helpful in taking future preventive actions is essential to address data breaches.

B. COMPARATIVE ANALYSIS OF INTERNATIONAL BREACH NOTIFICATION LAWS

Various jurisdictions have adopted different legal frameworks to enforce breach notification duties, and their notification requisites and thresholds are:

1. European Union (GDPR Article 33 & 34): GDPR requires data controllers to notify the supervisory authority of a personal data breach within 72 hours after the breach has occurred,[22] unless the breach is not likely to require competent authorities to adopt measures to safeguard the rights and freedoms of individuals. Customer notification is a must without undue delay in case of a likely high breach impact.[23]

2. United States (California Consumer Privacy Act—CCPA, Sec. 1798.150): The CCPA requires businesses to implement reasonable security procedures to protect personal data.[24] The statute is silent about personal data breaches, but consumers are given a private right of action to bring civil actions for statutory damages. Therefore, this puts enough pressure on businesses to notify data breaches, or the risk of facing litigation will always loom.

3. Australia (Notifiable Data Breaches scheme - NDB, Part IIIC of the Privacy Act 1988): NDB applies where there has been an eligible data breach, namely where personal information has been accessed, used, disclosed, modified or lost, or where an action has been taken involving the access, use, disclosure, modification or loss of personal information, and is likely to result in serious harm to the individual to whom the information relates.[25] Timely notification enables a quicker response and can help mitigate individuals' harm.

4. Philippines (Data Breach Notification Management System—DBNMS): DBNMS provides a simple and uniform manner of submitting Personal Data Breach Notifications and Annual Security Incident Reports. Personal data breaches and security incidents must be submitted through this site alone to ensure efficient and transparent processing.[26] The online submission of data breach notifications through this system ensures a faster and more transparent processing of notifications. It also promotes public transparency concerning personal data breaches.

C. ASSESSING GDPR'S PIONEERING ROLE IN DATA BREACH NOTIFICATIONS

As seen, the GDPR in Articles 33 and 34 has taken a meticulous approach to data breach notification. The statute mandates timely notification of breaches with certain conditions and a detailed requirement for the contents of the notification, ensuring that both the authority and the individuals are informed sufficiently to mitigate the potential impact.[27]This focuses on the importance of data protection and cooperation among EU member states. Similarly, Section 1798.150 of the California Consumer Privacy Act 2018 and Part IIIC of the Australian Privacy Act 1988 through the Notifiable Data Breaches Scheme 2017 stress accountability and enforcement for protecting personal data.[28] The Data Breach Notification Management System has centralized and digitalized the data breach notification process, ensuring efficiency and transparently publicizing the data breaches. This sets a benchmark for other jurisdictions to adopt online platforms for managing data breaches. Therefore, it can be said that the GDPR has taken a pioneering step in this regard.[29]

[22] General Data Protection Regulation (GDPR), Arts. 33, 34.
[23] Ibid., Art. 34.
[24] California Consumer Privacy Act (CCPA), Sec. 1798.150.
[25] Notifiable Data Breaches (NDB) scheme, Part IIIC of the Privacy Act 1988.
[26] Data Breach Notification Management System (DBNMS), National Privacy Commission (NPC), Philippines.
[27] General Data Protection Regulation (GDPR), Arts. 33, 34.
[28] California Consumer Privacy Act (CCPA), Sec. 1798.150; Privacy Act 1988 (Cth), Part IIIC.
[29] Data Breach Notification Management System (DBNMS), op. cit.

3. ESTABLISHING AUTHORITY FOR ENHANCED DATA PROTECTION SUPERVISION

A. CRITICAL ROLE OF SUPERVISORY AUTHORITIES IN DATA PROTECTION

Without a supervisory body, a massive void exists in protecting an individual's personal data. Supervisory bodies ensure the implementation of their respective country's data protection law and monitor and ensure data protection compliance. They likewise examine grievances concerning data breaches and penalize defaulting entities for violating data protection law. Without a national supervisory body, there are no well-established channels or mechanisms to guarantee the safe handling of personal data. This will most likely result in further data breaches and misuse of personal data. Additionally, there is a body that can investigate an individual's complaints if their rights are infringed. This erodes the public trust in digital services, which harms economic and social growth.

B. INTERNATIONAL FRAMEWORKS FOR DATA PROTECTION SUPERVISION

1. General Data Protection Regulation (GDPR) - European Union: Article 51 has mentioned about nominating the Supervisory Bodies responsible for each member state to monitor and ensure GDPR compliance among the public and advisory body that is in connection with legislation regarding the process of personal data protection.[30]

2. California Consumer Privacy Act (CCPA) - United States: CCPA does not have a supervisory authority like GDPR; however, they have the California Attorney General as an enforcement officer responsible for implementing and enforcing this data privacy. The Attorney General's office published guidance to assist businesses in complying with the law and safeguarding consumers.[31]

3. Personal Data Protection Act (PDPA) - Singapore: Sections 8 and 9 in PDPA provide for the nomination of the Personal Data Protection Commission as a data protection supervisory body to enforce the act, including the powers to discharge its functions, investigative, enforcement and advisory role to engage with all entities to ensure compliance with PDPA.[32]

C. EVALUATING THE EFFECTIVENESS OF GDPR'S SUPERVISORY AUTHORITIES

The GDPR approach is the best because of its thoroughness and detail in prescribing supervisory bodies' structure, powers, and independence. Article 51 of the GDPR obliges all member states to nominate such bodies and be independent of the executive branch of government, ensuring they are empowered to implement and enforce data protection law. The GDPR, with its elaborate features on the Supervisory Bodies, is a harmonized law for a significant economic area with the effect of uniform enforcement of data protection. The independence of the Supervisory Body of each member state from the executive branch of government and the wide investigative, corrective, and advisory powers spelled out in Articles 57 and 58 of the GDPR set high standards in data protection enforcement.[33] These powers of the Data Protection Supervisory Bodies promote organizational compliance and accountability while safeguarding the rights of individuals to privacy in the member states.

IV. CONCLUSION

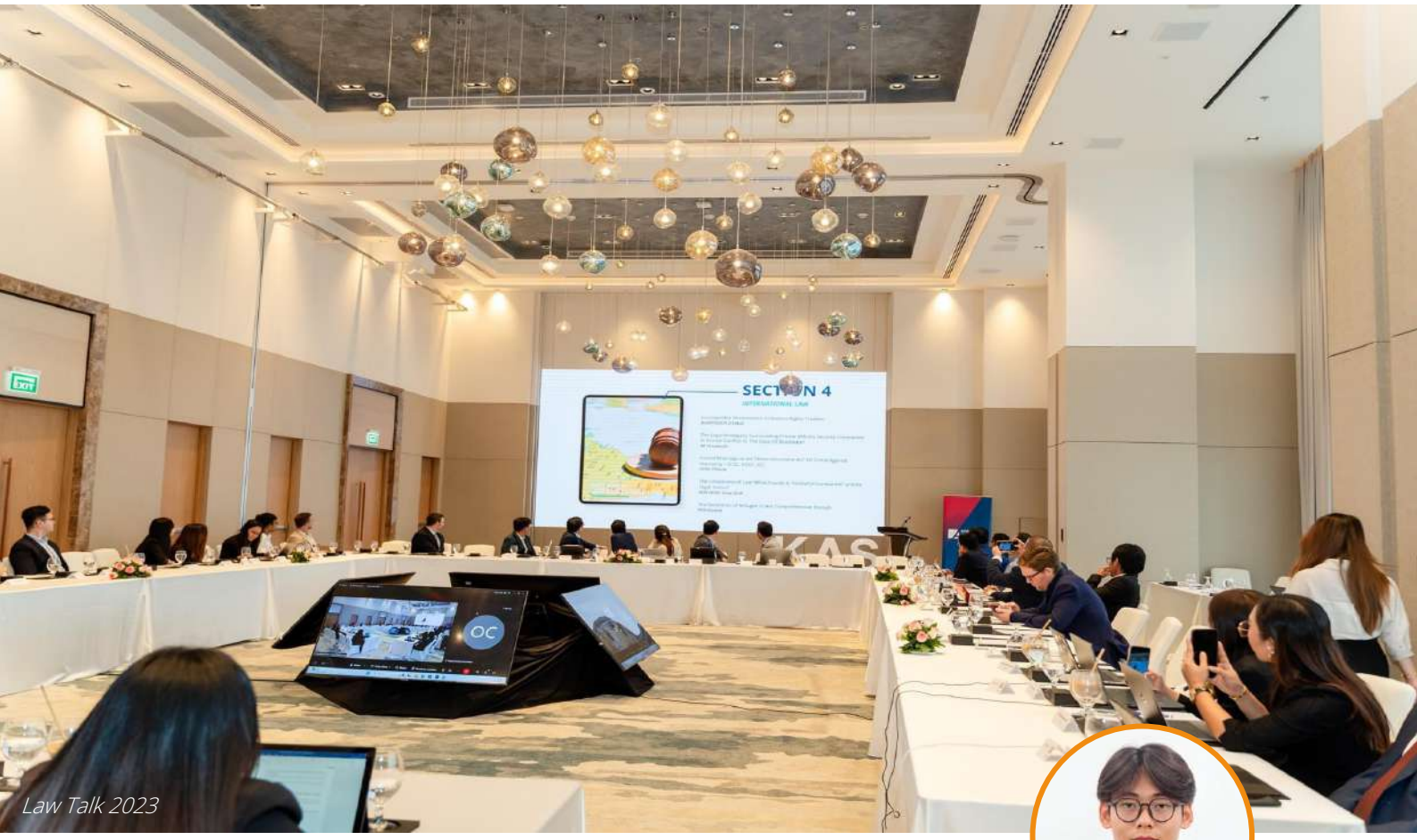
This legal brief examines possible options for strengthening corporate accountability in case of consumer data breaches that could happen in Cambodia. It proposes that Cambodia updates its existing legislative framework and put explicit and adequate legal measures in place to protect personal data, including in the digital economy. This legal brief notes that the European Union's General Data Protection Regulation, and most other global data protection laws and policies, often incorporate the following principles in solid legal frameworks to handle data breaches: transparency, accountability, and individual rights. Cambodia

[30] General Data Protection Regulation (GDPR), Art. 51.
[31] California Consumer Privacy Act (CCPA), Sec. 1798.150.
[32] Personal Data Protection Act (PDPA), Sections 8, 9.
[33] General Data Protection Regulation (GDPR), Arts. 57, 58.

should develop clear notification of data breach measures and explicit regulations on corporate accountability to protect the right to privacy and foster trust in the digital economy in Cambodia.

This law brief is necessarily tentative in many ways. While we provide detailed descriptions of the current challenges and proposed solutions for data protection in Cambodia, the proposed principles of reform—especially the GDPR-like ones—may not be the most appropriate or effective responses in the specific socio-legal context of Cambodia. Cultural norms, the economic system, and the level of technological development may affect the desirability and feasibility of some of the proposed reforms. Moreover, this brief does not engage in an in-depth inquiry into the practicalities of implementing and enforcing regulations, which may vary depending on sectoral regulations and the size of business operators.

Such recognition of limitations provides opportunities for future academic studies. Descriptions of the current status of Cambodia's digital economy could be undertaken with a longer view of how culture, economic systems, and levels of technology development may affect the desirability and feasibility of different legal responses. Comparisons with countries with similar cultural contexts, similar economic systems, and similar levels of development could provide insights into what legal solutions and mechanisms for enforcement would be effective in different sectors and of various sizes of business operators. Academic studies based on such descriptions and comparisons could then explore the practicalities of implementation and enforcement, including who should be involved, what capacity building is required, and what opportunities there are for inter-sectoral and inter-institutional coordination. Such knowledge would offer a more evidence-based understanding of possible pathways to effective data protection laws and policies in Cambodia.



Law Talk 2023

EXPLORING DATA PROTECTION OF THE DECEASED PERSON IN CAMBODIA

TOUCH Rattanak Raingsey

is a senior student in the English Language Based Bachelor of Law (ELBBL) at the Royal University of Law and Economics (RULE). In addition with the academic achievement, he participated in 30th Willem C. vis International Commercial Arbitration Moot, 3rd National Commercial Arbitration Centre Arbitration Moot Competition and with the academic experience as an advisor for Cambodia International Law Student Associate (ILSA). He has an interest with the commercial and corporate especially within the digital law theme and in addition with the interest in humanitarian international law.

I. INTRODUCTION

Cambodia has limited legislation, which is not comprehensive enough about personal data protection due to the law on personal data being at the drafting stage. Personal data protection provisions are available across specific statutes and constitutional law. The existing provisions related to personal data protection usually focus on the living individual, which leaves a gap for the protection of the deceased person and their digital data. Additionally, online platforms collect user data, especially when tailoring the advertisement for that specific user. That could also show that the user's personal data is unsafe since the company might collect more than their need for ad customization. Then, data that had been kept and used more than its original purpose, especially with the deceased person who cannot make a decision or have any legal capacity to dispute the issue. Therefore, the efficiency in data collection raises a concern for the user's privacy rights and underlines the necessity for government action to balance between the protection of the user's data and business driven by the use of personal data.

However, the law and regulations primarily focus on collecting and using data about living persons. This raises a question about the concern about the deceased person's data protection: what happens to the deceased person's data on the internet platform? Does the deceased person get protection from the law related to their data? Will the deceased person's data be kept with the online platform company or transferred to the succession of the dead person?

By examining these research questions, this research aims to assist with understanding and exploring the legal framework related to a deceased person's data rights on an online platform. This would involve data protection for the deceased person and the legal framework for succession in Cambodia.

II. CAMBODIA'S LEGAL CONTEXT PERTAINING TO DECEASED PERSON'S LEGAL CAPACITY

Generally, under the Cambodian legal perspective, the Cambodia Civil Code and Criminal Procedure Code of the Kingdom of Cambodia has a concept that a dead person will not have any civil or criminal liability since the dead person no longer has any legal capacity and existence.[1] Their legal capacity will be dissolved, and certain legal documents such as contracts and legal obligations will be terminated due to the parties being dead.[2] However, it does not mean that the dead do not have the right and protection under the law.

- Cambodia Civil Code 2007

Under Article 8, the dead person lost their legal capacity, which leads to being free from the obligation or any certain binding agreement such as the loan, marriage, adoption, buy and sale contract, service contract, or contract performance will be dissolved when one of the parties is dead except when it comes to the succession if the person dies, the commence of the succession by statutory or by testamentary is begin to enforce.

- Cambodia Intellectual Property Law, Law on Copyright and Related Rights

Article 19 states that the creator's moral right is permanent, which is perpetual; even if the creator is dead, the moral right of the product is still valid and still exists along with the work. This moral right provides credit to the creator with the protection of the creator's name to ensure that the creation has the creator's name.

Additionally, under Article 39, the economic right starts from the date of the creation of a work and is protected for 50 years following the creator's death. This means that financial earnings from the creation are still entitled to the creator's beneficiary for 50 years after the creator's death.

- Constitution of the Kingdom of Cambodia

In accordance with Article 31, Cambodia shall comply with the international human rights law and international human rights convention. Under the 1949 Geneva Convention, the additional Protocol of

[1] Article 8 of Cambodia Civil Code 2007; Article 7 and Article 24 of Criminal Procedure Code of Kingdom of Cambodia 2007.
[2] Article 8 of Cambodia Civil Code 2007.

1977 and Customary international humanitarian law also give a right to the dead person which the dead must be respected and protected to preserve their dignity while the corpse shall be handled with respect.[3] This shows that the dead person does not mean all of their rights are absolutely gone. There are certain rights that the dead person still has even though there are not many rights compared to the living person's rights. Also, all of these laws apply not only to the dead person but also to the living person in a way where the law limits the living person's right not to violate the dead person even if the dead person does not have equal rights to the living.

III. OWNERSHIP OF THE DECEASED PERSON'S DATA THROUGH SUCESSION LAW

Under Cambodian law, succession, as provided under the Cambodia Civil Code 2007, has two types: statutory and testamentary.

Statutory succession is a type of succession that is followed by the legal provision in which the family member can receive a piece of the asset of the dead person in the family through the law provision.[4]

The testamentary succession is the type of succession that respects the dead person's will and wishes that had been made during the time of the person alive, and the will gets notarized to be legit and enforceable.[5]

Moreover, the succession of the post or content made by the deceased person can be transferred to their beneficiaries or any third parties under the wish of the deceased person, especially the exclusive right or the economic right of the content from the deceased person.[6] The content is not just a digital asset. At the same time, it also contains the identities of the deceased person that show how they are identified on the online platform through their work or content, which can be considered personal data.[7] This would provide the legal framework for the beneficiaries to inherit the properties, especially the economic right of the property and the data through the succession legal framework under the Cambodia Civil Code.

In the case where there is a testamentary succession, this process makes a succession procedure less complicated and not difficult[8] since it would be easy for the successor to follow the will of the dead person by getting the information that the dead person had noted in their email, password and other necessary information to access the account to acquire the data for the successor as long as the will had been either notarize or there is a judgment from the court to enforce the will which is the requirement under the Cambodia Civil Code. However, in a case where the succession is a statutory succession of the digital data, it would be hard to find, especially in Cambodia, where the court case could not be accessed publicly, and it tends to be kept confidential.[9] Considering that Japan is the country that successfully helped Cambodia draft the Civil Code, these two countries' civil codes have a lot of similarities. [10] Additionally, the German civil code is the model code for these civil codes since during the drafting stage of the Japanese Civil Code, Japan chose the German civil code as their model law for drafting the code.[11] This will provide a brief legal matter on the digital data succession with the context of the deceased person's Facebook account and its data related to the legal matter addressed in the German court case. The Federal Court of Justice (Bundesgerichtshof, BGH), Germany's supreme court, decided that even Facebook had the term and

[3] International Committee of The Red Cross, "Humanity after Life: Respecting and Protecting the Dead", August 2019. Available at: https://www.icrc.org/en/download/file/117630/last_version_200583_respect_for_and_protection_of_the_dead_final.pdf
[4] Article 1145(2) of Cambodia Civil Code 2007.
[5] Ibid.
[6] Article 33 of Cambodia Law on Copyrights and Related Rights 2003.
[7] Luke Irwin, "the GDPR: What exactly is personal data?" , IT Governance European Blog, March 2022, Available at: https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data#:~:text=The%20GDPR%20further%20clarifies%20that,specific%20to%20the%20physical%2C%20physiological%2C
[8] Ratana Samnang, "Succession in Cambodia: Background, disqualification and Types", The University of Cambodia, Page.79. Available at: The Involvement of Youth toward Sustainable Development Goals (SDGs) in Cambodia (uc.edu.kh)
[9] Jay Cohen, Sochanmalisphoung Vannavuth, Chandavya Ing, "Cambodia-Data Protection Overview", 1.3 Case law, One Trust Data Guidance, October 2023. Available at: Cambodia - Data Protection Overview | Guidance Note | DataGuidance
[10] Tauchi Masahiro, "Becoming the Focal Point for Information Distribution on the Japanese Legal Assistance" ICD NEWS, Law for Development, July 2003.Page 2,3and 11. Available at: https://www.moj.go.jp/content/000111066.pdf ;
[11] Ibid.

policy that the deceased person's account will become the "memorialized account, " meaning no one can access or login to the Facebook account. Even Facebook provides a USB stick with a PDF file containing 14,000 pages, which is poorly structured and barely able to be read, which is deemed as not fulfilled by the court.[12] Therefore, the Federal Court of Justice decided that Facebook shall grant the dead person's account to her Parents (successor) to go into the account, not just receive the file of PDF, which is barely readable because the account and the data in the account are inheritable. This succession shall comply with the law, and the successor is entitled to the deceased person's data since there is no evidence that the child had any written letter stating that the data shall be deleted or the beneficiary is not entitled to her account. Therefore, her account shall be provided to her beneficiary under the succession law.

IV. LIMITATION FOR ASSESSCING THE DECEASED PERSON'S DIGITAL DATA ON THE ONLINE PLATFORM

The succession on the digital data on the online platform shall be limited since the right of the dead person which posts mortem privacy right of the deceased person exists, which means the succession shall be limited and stop at the borderline of the existence of a right of the deceased person and the transfer of the economic right under the copyright to the alive person to enjoy the benefit. Even the dead person also had the right to ensure their privacy because Article 40 of Cambodia's Constitutional Law concerns the right to privacy for every Cambodian citizen. This shows that privacy for Cambodian citizens always exists no matter what.

If we explore the international concept related to the deceased person's personal data rights, we can see that even though GDPR does not provide any protection to the deceased person, it encourages the member state to provide the ruling and regulation on that issue.[13]

Additionally, the ASEAN framework with the principle of personal data protection is not a binding regulation; however, it is persuasive for setting a standard for ASEAN members.[14] Under the legal framework, several principles could assist the deceased person's data to avoid any unfair treatment or exploitation of the data subject (deceased person).

Such "Retention" principle explains that the organization shall retain the personal data just enough to serve the purpose within a reasonable time, shall not extract an excessive amount of personal data than the need is and shall dispose of the personal data of the data subject when there is no longer reasonable to keep the data for legal or business purpose to avoid any exploitation.[15]

Overall, the right of the deceased person over their personal data is to provide dignity and privacy to ensure their sensitive data could be prevented from humiliation and respect their right and choice to keep what they wanted to be kept from other people. Additionally, with the assistance of the international legal framework and principles related to personal data, the deceased person's personal data could avoid any exploitation after they could not protect or prevent it.

V. CONSIDERATION: THE IMPORTANCE OF THE DEAD SWITCH BOTTON

Dead Switch Botton could be part of the solution that balances the interest of the living person and also the respect for the dead person based on their intention to handle the deceased person's personal data.

[12] Angelika Fuchs, "What happens to your social media account when you die? The first German judgements on digital legacy", ERA Forum, 10 September 2021, Available at: What happens to your social media account when you die? The first German judgments on digital legacy | ERA Forum (springer.com) Page3,5,6; Gesley, Jenny, "Germany: Federal Court of Justice Clarifies Scope of Postmortem Access to Social Media Accounts". 2020. Web Page. Available at: https://www.loc.gov/item/global-legal-monitor/2020-09-30/germany-federal-court-of-justice-clarifies-scope-of-postmortem-access-to-social-media-accounts/

[13] The Recital 27 of the General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/recitals/no-27/

[14] ASEAN Telecommunications and Information Technology Ministers Meeting "Framework on Personal Data Protection" Page4. Available at: https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

[15] Ibid

According to the Interest Theory, the person who is unable to make a choice as long as they have an interest they could be the right holder even if they cannot express the choice.[16]The dead person can be granted a de facto legal right that can be enforced against the living person when the law protects the interest of the dead person.[17] Due to the Interest theory approach to creating the posthumous right.[18] Therefore, providing a concept of a dead switch available in the mainstream online digital platform could assist with the legal framework for protecting the privacy of the deceased person's personal data.

An excellent legal framework cannot be created within a short time without any experience or complete contact with the issue; however, with the personal data legal framework, the government could learn from the non-government company policy and terms and conditions that could help set the standard for the data law protection of the deceased person. If we look at Meta company (Facebook) policy related to the deceased person, we can see that Meta has launched a policy to manage a memorialized account, which is the way to manage a deceased person's account through the legacy contact.[19] The rationale for the memorial account policy is to respect the choice of the person that had set before they are dead to a candidate in the legacy contact and to protect or prevent any fraudulent activities or any attempt to log in to the deceased person's account which could keep the account more secure.[20] Once the deceased person's account becomes memorialized, the word "Remembering" will appear above the name of the profile of the account, which later helps raise awareness that that person is no longer alive and could help the community from any fraudulent act or identity theft, as the legacy contact. This shows there won't be any access or succession of the deceased account for Facebook. All we can do is request to delete an account or certain post or post that is tagged to or related to the deceased person, which violates the deceased person's right or provides a bad picture or graphic to the deceased person.[21]

Google policy, which handles the deceased person's data, is called the inactive account manager, which is a way for account owners to share parts of their account data or notify someone if their account becomes considered inactive for a period of time since there is a choice for us to set up for the inactive period to consider as inactive which range from 3,6,12 or 18 months and before one month, the period that had been set for the account to be regarded as inactive google will contact the owner to notify before google start the procedure of inactive account manager.[22] However, the owner of the account also had a choice to delete the account if it became inactive.[23] In this feature, the account owner can also choose the data type to share with the trusted contacts in this feature.

After all, combining the rights of the deceased person and the dead switch could provide a baseline for protecting the deceased person's overall right to data. At the same time, the beneficiaries or any third parties with interest could receive a benefit and control over their piece of the deceased person's digital legacy with the balance of the deceased person's right and the beneficiaries' interest.

VI. CONCLUSION

In Conclusion, the deceased person should be put into more consideration within the scope of the data protection because certain rights related to the deceased person do exist, which makes the protection a need since a deceased person would be vulnerable to the wrong usage of their data without any consent or prevention from the deceased person when their data get use or when their identity got stolen and use to commit the crime which would likely affect the deceased person's dignity due to the crime happen

[16] Kristen Rabe Smolensky, "Rights of the Dead", Hofstra Law Review 2009, Vol.37 issue 3 article 4, Page 769. Available at: http://scholarlycommons.law.hofstra.edu/hlr/vol37/iss3/4
[17] Ibid Page 764
[18] Ibid Page774
[19] Help Center, "Managing a Deceased Person's Account"" Facebook. Available at: Managing a Deceased Person's Account | Facebook Help Center
[20] Transparency center, "Policy rationale", Meta, Available at: Memorialization | Transparency Center (fb.com)
[21] Transparency center, "Policy rationale", Meta, Available at: Memorialization | Transparency Center (fb.com)
[22] Google Account Help, "Inactive Account Manager" Google, Available at: https://myaccount.google.com/inactive?pli=1
[23] Ibid.

with their identity. In contrast, the dead person did not have any chance to commit the crime. The deceased person's data can benefit their beneficiary or the public. Still, its usage shall be limited to the dead person's dignity, privacy, and morals.

Cambodia needs a comprehensive digital law, especially regarding personal data protection. Since digital laws like personal data protection, cybercrime, and cyber security are still in the drafting stage, we could look into the existing laws to provide a provision related to personal data protection. Even though there is no comprehensive provision on the issue, a limited provision disregards data protection.

With an extension of existing guidelines from different jurisdictions to emulate, Cambodia shall consider those of the European Commission, ASEAN legal framework, and big online platform company guidelines owing to their compatibility with the current regulatory framework and the need to build towards the collective protection of not just a living person but also the deceased one.

MISTI's report focuses on Blockchain adoption for Cambodia's future growth.
Source: Khmer Times

CAMBODIA'S LEGAL FRAMEWORK FOR PRIVACY PROTECTION AMIDST THE INTEGRATION OF BLOCKCHAIN

MEY MONITA

is a Junior student majoring in the English Language Based Bachelor Program (ELBBL), the Royal University of Law and Economics (RULE), at the same time she is also a Junior student majoring in the Department of International Relations (DIR), Institute of International Studies and Public Policy (IISPP), Royal University of Phnom Penh (RUPP). On top of her studies, She is a legal intern at the Center for Advanced Research and Legal Studies (CARLS), Asian Vision Institute (AVI). She was the delegate representing the Republic of Malta of Phnom Penh Model United Nations 2023 (PPMUN), Royal University of Phnom Penh (RUPP). Besides involving her life in academics, she is a Vice President of Finance and Legality, at AIESEC in IFL. She is also one of the KASFLY Fellow 2024, and her fields of interest are Digital Law, International Issues related to countries' relations, and Digital Economics.

I. INTRODUCTION

The world is becoming a dramatic place where dependence upon technology and the IoT are becoming increasingly integral to people's livelihoods. Technological development has been innovation; perhaps the most exciting in recent years is Blockchain Technology's introduction. Blockchain is a form of digital technology used by professionals to store decentralized data, providing the stakeholders with absolute access to the data.[1] This is the newly developed idea of data storing, which offers benefits for many sectors such as the government, financial, medical, and banking sectors.[2] However, the dual nature of technology brings forth concerns regarding data protection that potentially threaten the individual's well-being. The data stored using blockchain technology is openly accessible to the relevant parties and is a potential threat to the Personal Data information owner.[3]

Alternatively, in Cambodia, the proper standard of data protection has yet to be established. As the announcement of the drafting Data Protection Law on 19 February 2021 by the Ministry of Post and Telecommunication ("MPTC"), the definition of Personal Data Protection is the information (names, identification, residence, email address, and phone number) that can identify their identity.[4] Meanwhile, General Data Protection Rights ("GDPR") protect the general data that can be used to determine the individual's identity.[5]

As a result, the MPTC is working on drafting a Data Protection law in Cambodia.[6] In addition, the Cambodian Constitution guarantees privacy rights under Article 40, which specifically addresses the issue of privacy protection in communication and residence. Still, it does not fully cover data protection on the digital scale.[7] Moreover, Article 10 of the Civil Code of Cambodia states that individuals are entitled to their rights, including life, personal safety, health, freedom, identity, and dignity.[8] In this general law, there is no special provision to mention Data Protection, which is not efficient enough to protect the Personal Data protection of each individual yet. Therefore, the legal issue will focus on the gaps in Cambodia's legal framework regarding Personal Data Protection. This will lead to an inquiry into practical standards for Cambodia to implement Personal Data Protection within the context of the increasing use of blockchain technology in the kingdom.

In this paper, we will explore Cambodia's areas for improvement in Personal Data Protection amidst blockchain integration by analyzing the standard of Personal Data Protection law and assessing criteria from international standards, primarily the standards of the European Union ("EU").

II. CAMBODIA'S LEGAL FRAMEWORK FOR PRIVACY PROTECTION

The prospect of Blockchain Technology integration has flowed in Cambodia's society, yet Cambodia's legal framework on Personal Data Protection is developing. The specific law that specifies Personal Data Protection needs to be more comprehensive in discussing modern technology, and it stays outside the standard to protect Data Protection compared to the standard of international Personal Data Protection laws. Concerning Data protection and comprehensive provisions, Cambodia's existing laws yet address this problem comprehensively, especially in the Internet of Things era.

The Constitution of Cambodia does not have laws to measure or scope Personal Data Protection rights.[9] Article 40 of the Cambodian Constitution articulates only about citizens' Data privacy protection, specifying

[1] Sopheap Ing, Vatana Chea, "DIGITAL INSIGHTS FUTURE of CITIES," BLOCKCHAIN TECHNOLOGY: A key Enabler of Future Smart Supply Chain Management, ed. Thomas Hesketh & Oudom Oum (Konrad Adaneur Stiftung, 2022), pp.72-80.
[2] Baker, Pam, "Today's Blockchain Use Cases and Industry Applications," SearchCIO, July 6, 2023, https://www.techtarget.com/searchcio/feature/Todays-blockchain-use-cases-and-industry-applications.
[3] Daniel Drescher, Blockchain Basics A non-technical Introduction in 25 Steps,(Apress, 2017), pp. 206-211.
[4] Jay Cohen, Sochamalisphoung Vannavuth, DATA PROTECTION LAWS of the WORLD Cambodia (DLA Piper, 2024), pp. 2-3.
[5] GDPR, Art. 1.
[6] Jay Cohen, Sochamalisphoung Vannavuth, DATA PROTECTION LAWS of the WORLD Cambodia, op. cit., p. 1.
[7] Cambodia Constitution, Art. 40.
[8] Civil Code Cambodia, Art. 10.
[9] Jay Cohen, Sochamalisphoung Vannavuth, Chandavya Ing, "Cambodia – Data Protection Overview," One Trust Data Guidance, October 2023, https://www.dataguidance.com/notes/cambodia-data-protection-overview.

"the rights to privacy of residence, and the secrecy of correspondence by mail, telegram, fax, telex, and telephone shall be guaranteed."[10] Discussion of privacy data under the Constitution is scoped only to the data privacy of residences and the secrecy of the data owner's response. This indicates that Cambodia's Constitution is limited and excludes the right to Personal Data Protection in a digital sphere.

Under the Civil Code of Cambodia, there is no provision for Data protection on the IoT. Still, it does state personal rights protection under Cambodia's Civil Code. Article 10 of the Civil Code states that individuals are entitled to their rights, including life, personal safety, health, freedom, identity, and dignity. Based on this Article of the Civil Code, people's fundamental rights are being protected. Still, it fails to mention the specific provision of Personal Data protection in the eco-digital system.

A gap exists in Cambodia's law regarding the practice of Perosnal Data protections, including a gap in measuring and ensuring technology safeguarding in the country. Verify. Gov.Kh was introduced in Cambodian in 2024; this platform was established by the Ministry of Post and Telecommunication (MPTC) to deliver convenience and easily accessible public service for Cambodian citizens to verify their official documentation, and all documents are stored in the Blockchain System.[11] This new initiative project provides extensive tools to Cambodian citizens. Still, the provision on Data Protection has not yet been introduced and specified in the law, which creates legal gaps in Personal Data Protection to ensure the safety of usage for the citizens; for example, all information in blockchain technology cannot be revokable,[12] which makes the owner's personal information unsafe. As a result, the right to erasure, one of the GDPR principles, plays a significant role in approaching the nature of blockchain technology. Therefore, the Personal Data Protection law is a shield in strengthening blockchain technology.

Overall, Cambodia's legal framework lacks Personal Data Protection provisions, while the existing laws of the EU provide the foundation elements of Personal Data Protection that are important for blockchain integrations.

III. INTERNATIONAL STANDARD OF PRIVACY PROTECTION: GENERAL DATA PROTECTION OF THE EUROPEAN UNION'S BLOCKCHAIN APPLICATION

The EU's GDPR provides a comprehensive framework for practicing Data protection. It established the safeguards atmosphere to protect citizens' data and created the standards of Data protection that prevent threats to public security, especially the integration of Technology.[13] If compared to Cambodia's legal framework in practicing data protection, Cambodia has a gap for improvement following GDPR's standard.

Regarding Blockchain Technology, the EU wants to have a lead role in this technology and be a significant factor in finding the applications or platforms.[14] As the originator of GDPR, the EU must ensure that digital identity and data protection are under observation and comply with the law during the flow of blockchain.[15] For the Blockchain application, the EU plans to implement "Building a pan-Europe public services blockchain" and "European Blockchain Sandbox."[16] Yet, they face legal considerations on data protection and question the safety of the usage of these applications.

The European Union takes GDPR so seriously that those applications must comply with the Personal Data Protection standard. This law enshrines the right of an individual to protect his data from any party as a fundamental principle.[17] Personal Data protection rights have principles for data protection in processing,

[10] Cambodia Constitution, Art. 40.
[11] "Press Release on Cambodia's VERIFY.GOV.KH Document Verification Platform Wins Gold in ASEAN Digital Awards 2024," PRESS OCM I, February 2, 2024, https://pressocm.gov.kh/en/archives/90360.
[12] Daniel Drescher, Blockchain Basics A non-technical Introduction in 25 Steps, op.cit., pp. 206-211
[13] General Data Protection Rights ("GDPR"), Art 1.
[14] "Blockchain Strategy | Shaping Europe's Digital Future," European Commission, February 27, 2023, https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy.
[15] "Blockchain Strategy | Shaping Europe's Digital Future," op. cit.
[16] Damvakeraki, Tonia, EU BLOCKCHAIN STRATEGY, (EU Blockchain Observatory and Forum April 25, 2024), pp.7-8.
[17] GDPR, Art. 8(1) & Art.16(1).

including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.[18] In addition, GDPR provides the user with the right to data erasure. The user can possess control of their data and can delete the data concerning her without delay, which is essential in protecting users' personal information if there is information that can intervene the individual's personal Data.[19] Additionally, the right to rectification is also stated under GDPR.[20] This right allows the replacement of incorrect data with the correct data under the authority of the Data controller; the inaccuracy of data is essential; thus, it will harm the Personal data of the individual and have a long-term effect on the individual. Besides the right to erasure and the right to rectification, the right to data portability is also provided under GDPR.[21] This right gives access to the individual in receiving their personal information that the controllers have stored. The rights provided under GDPR give the user the right to control their own data with the authority of the Data Controller or the Data processor.

Moreover, GDPR emphasizes Data Breaches where the controller has to provide notification within 72 hours or to the supervisory Authority about the breaches.[22] Under GDPR, the Data Controller is the legal person, natural person, agency, or public authority who joins to determine the purpose of processing personal data protection. A data processor is a legal person, natural person, agency, or public who processes Personal data protection. These two actors in GDPR have different roles in doing their work regarding data protection, which is essential in processing data protection in the country. This can ensure the user's safety within the data breach time frame and prevent any data breach.

While the application set out by the EU requires the user's data to be stored, the concern is that GDPR is very strict about complying. GDPR is the standard that the application needs to compromise; it created a safe place for data protection in the European Union concerning the region's high level of data protection.[23]

The GDPR's application in Cambodia's case is a solid model. However, the uniqueness of Cambodia's social and contextual landscape in Southeast Asia poses obstacles to the full adoption of the international standards of Personal Data Protection Rights in accordance with GDPR. Nevertheless, the GDPR is one of the best examples that give Cambodia a beneficial framework, especially in creating Personal Data Protection regulations designed explicitly for Blockchain technology.

IV. BENCHMARKING CAMBODIA'S LEGAL FRAMEWORK AND EU'S GDPR

The law benchmarking between Cambodia's legal framework and GDPR showed a gap in development in Cambodia's framework; thus, the substantial elements in GDPR's Data Protection will fill that gap. The Cambodian Constitution and Civil Code are limited in discussing protecting Personal Data in the digital sphere.

As a developing country with a civil law system, Cambodia's current social context does not offer robust data protection, potentially compromising individual safety. Adopting and aligning with international Personal Data Protection standards can yield substantial benefits, including economic growth, enhanced international exposure, and improved living standards.

The introduction of new technologies and strong data protection measures would attract foreign visitors and investors, boosting Cambodia's economy and enhancing citizens' quality of life. The reliability of the Personal Data Protection framework would position Cambodia positively internationally, ensuring data protection for residents and visitors.

The comparison of Cambodia's Personal Data protection with the EU's GDPR highlights areas in which Cambodia can improve. Several vital points will be addressed to enhance and strengthen Personal Data

[18] "What is GDPR, the EU's New Data Protection Law?" GDPR.eu, September 14, 2023, https://gdpr.eu/what-is-gdpr/.
[19] GDPR, Art. 17.
[20] GDPR, Art. 16.
[21] GDPR, Art. 20.
[22] GDPR, Art. 33.
[23] InterSoft Consulting. 2013. "General Data Protection Regulation (GDPR)." General Data Protection Regulation (GDPR), 2013, https://gdpr-info.eu/art-1-gdpr/.

Protection in the Kingdom and ensure efficient data protection practices. The limitation of the Constitution of Cambodia and the Civil Code only discusses privacy protection in the digital sphere, which lacks the principle of data protection and deters users from using their rights in a way that can benefit the data's users.

The absence of a Personal Data Protection Principle in Cambodian law reveals a significant gap in the country's data protection practices. In contrast, the GDPR clearly outlines these principles and defines their roles, making it straightforward to apply them in data protection. Cambodia's Civil Code addresses individual living rights, and the lack of specific Personal Data Protection principles results in a lack of guidelines for governing digital protection practices. This weakens Cambodia's framework, clarifying which principles should be used in data protection. Therefore, adopting a principle similar to the principle of GDPR is a critique in Cambodia; thus, it ensures the safeguarding space for using innovative technology called Blockchain Technology.

The GDPR reflects users' rights in controlling personal data protection and designates the exact timeframe for notification of data breaches. On the other hand, Cambodia's Constitution and Civil Code only stipulate individual rights but fail to give a precise mechanism for data breach notification. Due to these gaps, it is highly challenging for Cambodia to implement applications related to data protection practices, including blockchain integrations. The GDPR is very strict and an ideal standard and Cambodia requires a robust framework to follow. Consequently, users in Cambodia cannot wholly exercise their rights in data protection, such as the right to erasure, which is meant to eliminate unnecessary data threats as described in the GDPR.

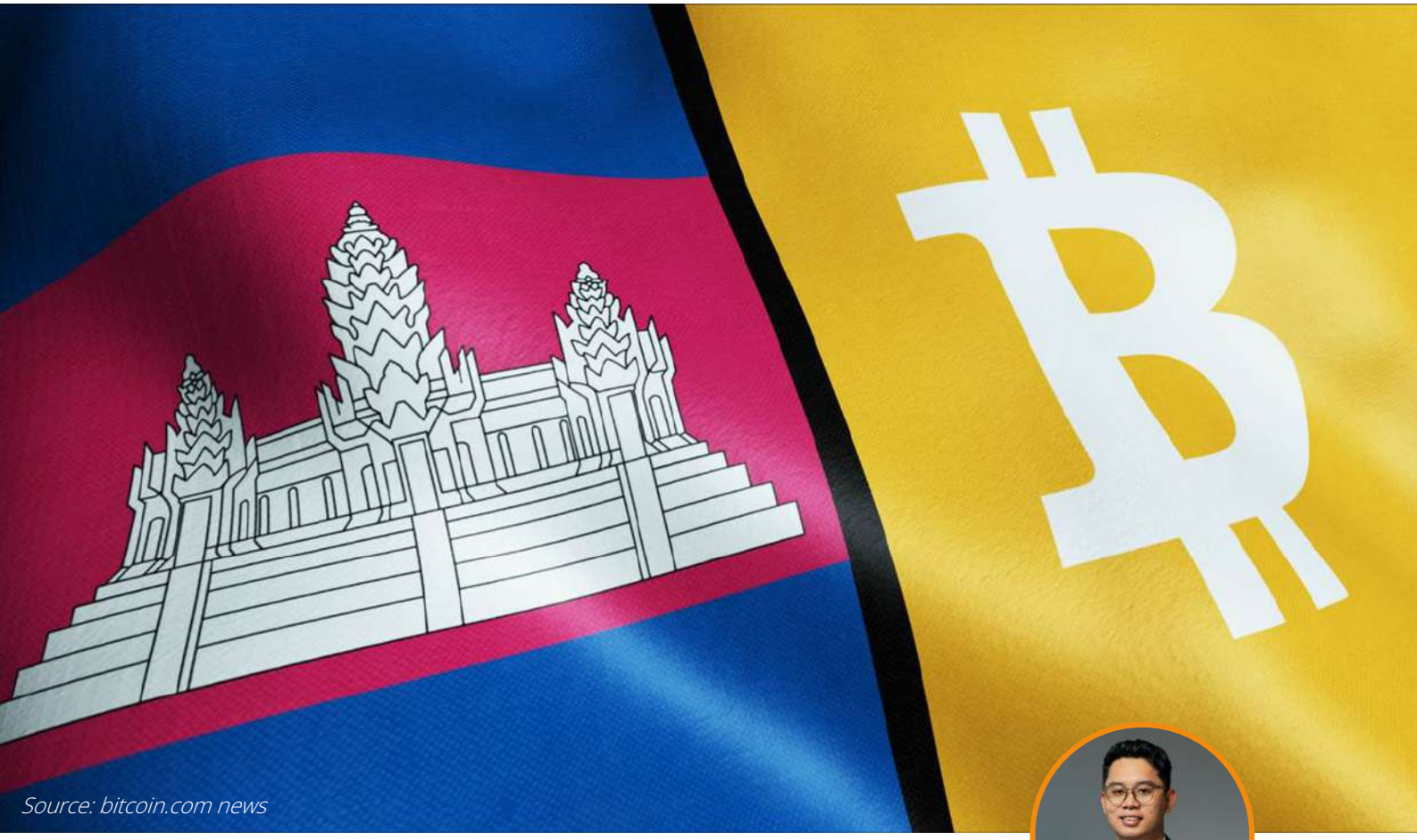
The lack of proper implementation has challenged Cambodia to provide data protection by integrating blockchain technology for data security. Cambodia needs to clearly define the scope of protection in the aspect of the Personal data to solve the problem of lack of regulation. Verify.Gov.Kh is a leading platform where Cambodians can securely store data using blockchain technology. However, the emergence of unforeseen issues with the Internet of things might challenge it. Similarly, Cambodia needs a relevant law to regulate Verify.Gov.Kh. It should be another layer of protection for individual personal data, given the fact that it is a public platform in the country. Therefore, to solve the problem of internet threats, there is a need to set a robust framework for the protection of personal data that will consider data processing principles and users' rights and protect the ecosystem.

V. CONCLUSION

To conclude, the benchmarking between the GDPR of the EU and Cambodia's legal framework showed a significant improvement for Cambodia toward the journey of precise regulation in practicing the Personal Data Protection field. As technology keeps integrating, Cambodia has introduced blockchain applications into the country as the official platform that can help improve citizens' lifestyles to be better. However, the absence of special provisions on digital law threatens the safety of the citizens in cyberspace, especially during the integration of modern technology. The long journey of practicing requires action from experts in technology along with the existence of international standards as the end goal for Cambodia to take as a model. The vast digital space and a keen interest in learning and developing for practicality and legality could change Cambodia greatly. The rule of law is a requirement to govern society and make space for everyone in the country and the world. As Cambodia is currently drafting a Data Protection law, there would be a fruitful outcome with that law. The measurement and providing of knowledge of personal data protection shall be spread to Cambodia.

However, with this law brief, we hope to catalyze lawmakers to think from another perspective about how blockchain and data protection are related. The legal framework alone will not make data protection successful; thus, public awareness and contributions will mark the success of data protection in the Kingdom.

Section 2
Digital Law and Fintech



Source: bitcoin.com news

FROM SANDBOX EXPERIMENT TO CRAFTING THE REGULATION: THE CASE FOR CRYPTOCURRENCY FRAMEWORK IN CAMBODIA

PRUM Sopheareach

serves as a legal assistant at SOK SIPHANA & ASSOCIATES, where he primarily supports and advises various growing sectors within the Cambodian economy. He earned a Bachelor of Laws (LLB) from the Royal University of Law and Economics (RULE) and a Bachelor of Arts (BA) in International Relations from the Institute of Foreign Languages (IFL). During his academic journey, he participated in the prestigious Philip C. Jessup International Law Moot Court Competition as both a mooter and co-coach, working on legal memorial involving claims such as Digital Human Rights and Cybersecurity Law. His research interests encompass FinTech, Energy, Investment, and Capital Markets.

I. INTRODUCTION

In recent years, Cambodia has seen a growing interest in cryptocurrencies, with individuals and businesses exploring their potential for investments, transactions, and financial innovations.[1]

Regulators currently face challenges in incorporating cryptocurrencies into existing frameworks due to their decentralized structure and borderless transactions.[2] Unlike traditional currency, these new forms of assets are not backed by tangible assets recognized by authorities and have not yet received official government recognition.[3] Meanwhile, in Cambodia, a joint statement issued by NBC, SERC, and the General Commissariat of the National Police in 2018 declared it illegal to spread, circulate, buy, sell, trade, or settle cryptocurrencies without obtaining a license from the appropriate authorities.[4]

While there is not a fully-fledged legal framework yet, as of January 2024, the first digital asset exchange in the country is permitted to operate within the Fintech regulatory sandbox established by the SERC.[5] Meanwhile, the NBC has enforced a resolution that effectively bars all banks and financial institutions from engaging in any cryptocurrency-related activities, a stance that has remained unchanged since 2017.[6] With initiatives from SERC, it can be safely stated that the RGC is moving towards implementing a more robust regulatory framework and is becoming more open to allowing some crypto transactions to take place in Cambodia.

This paper will assess the current regulatory framework in Cambodia. Initially, a comprehensive evaluation will be carried out to analyze the regulatory measures developed by various concerned jurisdictions that are considered proactive in regulating Fintech products. This assessment will aim to identify and emphasize similarities and differences across these countries. Furthermore, insights will be provided through the analysis, along with recommendations tailored for the legislative framework governing Cambodia's cryptocurrency space.

II. LEGAL ISSUE

In the regulatory realm of Fintech in Cambodia, cryptocurrencies reside in an area not governed by the existing legal framework. In the banking sector, Prakas No. B14-107-161 serves as the existing regulation allowing the transaction of digital assets, specifically electronic money.[7] Under the watchful eye of NBC, the financial institutions are categorically barred from engaging with any crypto related-business.[8]

However, amidst this stringent oversight from NBC, the recent issuance of Guideline No. 009/23,[9] adopted by SERC in line with Prakas No. 037, [10] suggests a new approach toward promoting and testing cryptocurrencies. The regulatory sandbox provides a controlled setting where companies can test their new financial products with real customers for a limited time and within specific parameters. This allows them to experiment before fully launching their products on a larger scale.[11]

This platform serves as a "test and learn" mechanism, enabling businesses to trial Fintech products without obtaining a license. However, it is designed for a limited duration and with restrictions, usually for

[1] "Royal Group Exchange: Embarks on a Path to Transform Cambodia's Crypto Landscape with Localized, Regulated Approach" Cambodia Investment Review 2024. January 23, 2024. https://cambodiainvestmentreview.com/2024/01/23/royal-group-exchange-embarks-on-a-path-to-transform-cambodias-crypto-landscape-with-localized-regulated-approach/.
[2] Sotiropoulou, Anastasia, and Stéphanie Ligot. "Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?." European Company and Financial Law Review 16, no. 5 (2019): 652-676., p.9.
[3] Venter, Henri. "Digital currency–A case for standard setting activity." A perspective by the Australian Accounting Standards Board (AASB) (2016): p.5.
[4] NBC, SERC and the General-Commissariat of National Police, "Joint Statement", 16 January 2018, 2.
[5] "Exploring RGX: An In-Depth Look at Cambodia's First Licensed Digital Asset Exchange." B2B, January 31, 2024. https://www.b2b-cambodia.com/articles/exploring-rgx-an-in-depth-look-at-cambodias-first-licensed-digital-asset-exchange/.
[6] NBFSA, Resolution No. ន. 7 017 108 to All Banks and Micro-Finance Institutions in Cambodia to Ban the Trading of, Sale, and Advertisement of Cryptocurrencies and Similar Digital Assets That Was Not Recognized By NBC, 05 December 2017.
[7] NBC, Prakas No. B14-107-161 on the Management of Payment Service Providers, 14 June 2017, art.5.
[8] Resolution No. ន. 7 017 108, 2017.
[9] SERC, Guideline No. 009/23 on the Regulatory Sandbox in Securities Sector, 07 August 2023.
[10] NBFSA, Prakas No.037 on FinTech Regulatory Sandbox in Non-Bank Financial Services Sector, 04 August 2023.
[11] Guideline No. 009/23 on the Regulatory Sandbox in Securities Sector, 2023, p.1.

testing purposes. Once the testing period is over, there may not be clear guidelines on transitioning to full-scale operations and implementing ongoing regulatory compliance. One could say that the current Guideline No. 009/23 favors a principles-based approach over a prescriptive, rules-based one. Given that cryptocurrency is not governed by either banking or securities sector regulations, it is necessary to establish a bespoke framework and determine which regulatory body should implement these regulations.

III. LEGAL IMPLICATIONS

Cryptocurrencies pose a unique set of challenges, which makes designing the personal scope and content of regulation very difficult. If Cambodia builds a bespoke framework, the Cambodian regulator ("Regulator") should consider the following points.

Firstly, a common definition of cryptocurrency should be adopted. Secondly, CASPs should establish adequate governance and organizational arrangements and comply with the licensing requirements set by the regulator. Thirdly, CASPs should establish adequate arrangements to protect against the risks of users' assets in their custody. Lastly, CASPs shall comply with the AML/CFT measures that are in place.

1. DEFINITION AND CATEGORIZATION

Firstly, defining the legal characterization of cryptocurrency is challenging due to the combination of characteristics of currencies, commodities, payment systems, and securities.[12] Their classification in one category or the other will dictate their regulatory status. We can find a suitable definition of cryptocurrencies based on an analysis of definitions ranging from broad to strict.

Jurisdictions	Level of stringent	Definition
2023 EU's MiCA	Broad	A crypto-asset is defined as a "digital representation of value or rights, which can be transferred and stored electronically, using a distributed ledger or similar technology".[13]
2019 Japan's PSA	Strict	A crypto-asset is defined as: "(1) a proprietary value that may be used to pay an unspecified person the price of any goods purchased or borrowed, or any services provided, where the proprietary value may be: (i) sold to or purchased from an unspecified person, provided the sale and purchase is recorded on electronic or other devices through electronic means; and (ii) transferred through an electronic data processing system; or (2) a proprietary value that may be exchanged reciprocally for the proprietary value specified in point (a) with an unspecified person, where the proprietary value may be transferred through an electronic data processing system."[14]
2020 Singapore's PSA	Stricter	Digital token refers to "any digital representation of value that (i) is expressed as a unit;

[12] Sotiropoulou, Anastasia, and Stéphanie Ligot. "Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?." op.cit., p.8.
[13] EU, MiCA Regulation, 31 May 2023, art.3.
[14] FSA, Japan's PSA, 31 May 2019, art.2.

		(ii) is not denominated in any currency and is not pegged by its issuer to any currency; (iii) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or the discharge of a debt; (iv) can be transferred, stored, or traded electronically; and (v) satisfies such other characteristics as the Authority may prescribe"[15]

As can be seen, the catch-all definition of crypto-assets, such as MiCA, is broadly and inclusively defined, capturing not only cryptocurrencies. We can observe under Japan's PSA and Singapore's PSA that crypto-assets have a dual function: they act as both a medium of exchange and an investment vehicle. The definition of crypto-assets in Japan's PSA is strictly defined, specifying various scenarios and conditions in which the crypto-asset can be used. Conversely, the definition from Singapore's PSA is stringent, detailing particular characteristics with open room for other characteristics to be prescribed by the authority. The conclusion that can be drawn is that there is no generally accepted definition of the term "cryptocurrencies" available in the regulatory space.[16]

Criteria	EU's MiCA	Japan's PSA	Singapore's PSA
Digital representation of value	✓	✓	✓
Transferable and storable electronically	✓	✓	✓
Use DLT or similar technology	✓	×	×
Recording on electronic devices	✓	✓	✓
Pegging to any currencies	×	×	✓
Medium of exchange	×	✓	✓

These jurisdictions may adopt various terms but have the same elements. However, comparing the definitions has raised critical remarks, requiring more detailed specifications of the various crypto-asset sub-categories and their scope. This is done with the view to drawing a clear distinction among these sub-categories, especially due to uncertainties raised by hybrid tokens, those crypto-assets performing different functions.[17]

For example, MiCA categorized crypto-assets into three types, subjecting to different requirements based on their associated risks:

1. Asset-Referenced Tokens are crypto-assets that aim to stabilize their value by referencing any other value, right, or combination thereof (e.g., commodities), including one or more official currencies.
2. Electronic Money Token is a type of crypto-assets that also aim to stabilize their value by referencing the value of a single official currency such as Euro or United States Dollars.

[15] MAS, Singapore's PSA, 28 January 2020, 2.
[16] Prof. Dr. Robby HOUBEN, "Cryptocurrencies and Blockchain – Legal Context and Implication for Financial Crime, Money Laundering and Tax Evasion" (European Parliament , July 2018), https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf, p.22.
[17] European Central Bank, "Opinion of European Economic and Social Committee on a proposal for a regulation on Markets in Crypto-assets and amending Directive (EU) 2019/1937)" Official Journal of the European Unio C 152, 1-9. (2021), 2.

3. Other Crypto-Assets are a category that falls outside the two types above and encompasses all other types of crypto-assets such as crypto-currencies like Bitcoin, Ether, etc.[18]

2. REGISTRATION AND OBLIGATIONS OF THE CASPS

A particularly important related question is: who should bear responsibility if things go wrong? Due to the decentralized nature of cryptocurrencies, regulators cannot directly pinpoint a central authority responsible for administering the system and offering redress.[19] Instead, one can regulate all those entities that provide cryptocurrency services. Users often rely on these intermediaries when they want to enter or exit the cryptocurrency market unless they find bilateral counterparties.

A. LICENSING REQUIREMENTS FOR THE CASPS

- MAS – Financial and Business Conduct's Requirements

MAS is the sole regulator governing the cryptocurrency market in Singapore, requiring entities to obtain a payment institution license.[20] CASPs are subject to two types of licenses: a standard payment institution license and a major payment institution license.[21] The decisive aspect of selecting a suitable license is the monthly transaction volume. Companies that conduct cryptocurrency transactions above USD 3 million per month are obligated to acquire a major payment institution license, while companies with lower cryptocurrency trading volumes are only obliged to obtain a basic payment institution license.[22]

To obtain the license, an applicant must maintain a minimum capital of USD 100,000 if applying for a standard payment institution license or USD 250,000 if applying for a major payment institution license.[23] Further, an applicant shall not be licensed unless:

(a) being a company incorporated in Singapore or overseas;

(b) having either a permanent place of business, a registered office in Singapore; and

(c) having at least one executive director who is a Singapore citizen or Permanent Resident. [24]

- FSA– Financial and Business Conduct's Requirements

The FSA requires only stock companies or foreign CASPs with offices in Japan to apply for a license. Among other requirements, applicants must also have a sufficient financial basis, with a minimum capital amount of JPY 10 million (approximately USD 64,000) and positive net assets.[25] Furthermore, the applicants are also required to have:

(a) a representative person in Japan (limited to a person domiciled in Japan);

(b) a satisfactory organizational structure and systems to provide the exchange services appropriately and properly; and

(c) certain systems to ensure compliance with the applicable laws and regulations.[26]

Additionally, the FSA requires applicants to complete a checklist of approximately 400 questions to verify that they have properly established systems to conduct service.[27]

---

[18] MiCA, 2023, art.3.
[19] Sotiropoulou, Anastasia, and Stéphanie Ligot. "Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?." op.cit., p. 9.
[20] Ikigailaw. "Cryptocurrency Regulation in Singapore: Challenges and Opportunities Ahead." www.ikigailaw.com, November 11, 2020. https://www.ikigailaw.com/article/231/cryptocurrency-regulation-in-singapore-challenges-and-opportunities-ahead.
[21] Singapore's PSA, 2020, 6.2.
[22] Singapore's PSA, 2020, 6.5(ii)
[23] Singapore's PSA, 2020, 6.15.
[24] Singapore's PSA, 2020, 6.8
[25] Arora, Gaurav. "Cryptoasset Regulatory Framework in Japan." Available at SSRN 3720230 (2020): p.2.
[26] Japan's PSA, 2019, art. 63-3.
[27] Arora, Gaurav. "Cryptoasset Regulatory Framework in Japan." Available at SSRN 3720230 (2020): p.3.

- Recommendations

Criteria	MAS	FSA
Monthly transaction volume	✓	×
Registered business	✓	✓
Representative in the country	✓	✓
Executive director	✓	×
Minimum Base Capital	✓	✓

Based on the information provided, there are no unified licensing requirements. However, Regulator could establish criteria regarding the type of legal entity, minimum directorship, and minimum base capital, varying depending on the type of licenses sought. They could also implement standards similar to those applied to traditional financial companies.

Regulator should design a tailored set of requirements based on a thorough study and analysis of Cambodia's market. For instance, regulations governing large-scale cryptocurrency exchanges may require more stringent capital requirements and risk management practices than regulations for smaller-scale wallet providers. This approach ensures the establishment of a robust framework, enabling service providers to conduct their operations reliably and appropriately.

B. REGULATORY OBLIGATIONS ON THE CASPS

- MAS – Supervision over Business Conduct

To promote transparency, MAS mandates that licensees must provide any information related to their operation of payment services as prescribed.[28] While this transparency obligation encompasses all matters, CASPs are often mandated to disclose information to MAS regarding their operations and the pricing of any services they offer.[29] These obligations are enforceable despite any potential privileges or secrecy requirements.[30]

Once granted the license, applicants are required to fulfill certain notification obligations, requiring them to inform MAS in the event of specific occurrences (e.g., any event that impairs the operation of the licensee, the licensee being unable to meet any of the licensee's financial obligations, or any significant change to the company's structure).[31] Furthermore, CASPs shall submit periodic reports related to the business to the MAS in frequency as the MAS may specify.[32] As an additional precaution, MAS required major payment institutions to maintain a specified monetary security amount with MAS or its equivalent in a foreign currency to fulfill their performance to users.[33]

- FSA - Supervision over Business Conduct

For supervisory purposes, CASPs are required to maintain books and documents on their services,[34] written reports on the amount of user's money and volumes of users' virtual currency under the management of service providers accompanied by financial documents and a certified public accountants

[28] Singapore's PSA, 2020, 16.
[29] Singapore's PSA, 2020, 16.
[30] Singapore's PSA, 2020, 16.3.
[31] Singapore's PSA, 2020, 15.
[32] Singapore's PSA, 2020, 17.
[33] Singapore's PSA, 2020, 22.
[34] Japan's PSA, 2019, art.63-13.

or audit firm's audit report on such documents.[35] FSA also has the authority to order a service provider to take necessary measures to improve its operations as required for supervision.[36]

- Recommendations

Establishing notification requirements can compel CASPs to uphold a minimum level of transparency with the Regulator. The Regulator may require licensees to deliver comprehensive details concerning their payment services operations and pricing to ensure transparency. More importantly, requiring CASPS to adhere to stringent notification requirements ensures that the Regulator remains informed about significant events, while regular submission of business reports helps to keep them updated.

To impose a financial requirement, the Regulator may authorize CASPs to provide a designated amount of security to ensure the fulfillment of their obligations. By imposing this security requirement and holding custody of these securities, the Regulator effectively enables exchanges to reimburse customers if the CASPs cancels its license or if the license is revoked. The Regulator may utilize the security to settle any outstanding claims made by the CASP's customers. Consequently, customers may recover portions of their outstanding claims against the CASPs. However, this security measure is not intended to, nor can it, provide complete insurance against all losses. Doing so would necessitate an impractically high-security deposit that would make the business financially unfeasible.

C. MITIGATING RISKS

- MAS – Consumer Protection Measures

MAS requires the CASPs to safeguard customers' assets.[37] The CASPs should ensure that the digital payment token instruments relating to at least 90% of the customer's assets (which have been deposited in a trust account(s) are stored at all times in systems that are not connected to the Internet or any other form of wireless communication ("cold wallets")[38], while the other 10% to be kept in other wallets ("hot wallets").[39]

Additionally, MAS required CASPs to segregate customers' assets and deposit them into a trust account for their benefit, maintain accurate books and records, and establish effective systems and controls to safeguard the integrity and security of customers' assets.[40] MAS recently unveiled comprehensive measures in its proposed regulation to mitigate potential consumer harm. MAS plans to issue detailed guidance for CASPs as part of consumer access measures. This involves assessing a customer's risk awareness and refraining from incentivizing crypto trading. Importantly, CASPs are required to implement complaints-handling procedures for retail customers.[41]

- FSA – Consumer Protection Measures

Japan's PSA also lists several consumer protection-focused standards for CASPs to meet on an on-going basis after being licensed. These requirements encompass:

1) implementing measures to safeguard customers' personal data;

2) providing new users with essential information, including the exchange's legal identity, registration details, potential risks associated with cryptocurrency, and clarifying that cryptocurrency isn't backed by the Japanese government or any other fiat currency;

[35] Japan's PSA, 2019, art.14.
[36] Japan's PSA, 2019, art.63-16.
[37] Singapore's PSA, 2024 Amendment, 18G.
[38] MAS, Guidelines On Consumer Protection Measures By Digital Payment Token Service Providers, 2 April 2024, 3.4.; Claire Huang, "What Crypto Consumer Protection Rules Are There in the World?," The Straits Times, July 21, 2023, https://www.straitstimes.com/business/what-crypto-consumer-protection-rules-are-there-in-the-world.
[39] David Heywood, "Crypto Asset Segregation and Custody Regulations to Go Live in October," Bovill, July 25, 2023, https://www.bovill.com/asia/crypto-asset-segregation-and-custody-regulations-to-go-live-in-october-2023/.
[40] Singapore's PSA, 2024 Amendment, 18B.
[41] Peiying Chua, "Securing the Future: MAS Unveils Final Consumer Access and Other Regulatory Measures for Digital Payment Token Services," Passle, November 27, 2023, https://techinsights.linklaters.com/post/102ituh/securing-the-future-mas-unveils-final-consumer-access-and-other-regulatory-measu.

4) segregating customers' assets from the exchange's assets and subjecting this segregation to audits conducted by certified public accountants or audit firms; and

5) establishing internal management systems to effectively address and respond to customer complaints in a fair and appropriate manner.[42]

- Recommendations

Based on the above, consumer protection requires considerations of both the provision of sufficient information to users and the protection of user assets.

As a precaution, CASPs will be mandated to communicate crypto-assets characteristics and contract terms to safeguard users clearly. Additionally, taking into consideration that some customers engaging in such trading may lack sufficient understanding of the risks involved in these products, it is deemed appropriate to require CASPs to refrain from engaging in misleading advertising, false announcements, or inappropriate solicitations. CASPs should not be allowed to use advertisements and solicitations that encourage speculative trading, thus promoting a more transparent and responsible environment for cryptocurrency transactions.[43]

To protect customer assets, Regulator can set the limit for which the proportion of customer assets could be held in the cold wallets. Cold wallets, being disconnected from the internet, are less susceptible to cyber theft, making this measure crucial from a cybersecurity perspective.[44] Another regulatory consideration involves mandating the segregation of customer assets from those of CASPs. Regulator can require CASPs to maintain customer assets in distinct blockchain addresses separate from their own assets. This entails depositing customer assets into a trust account and ensuring operational independence of the custody function.[45]

To create a dispute resolution mechanism, CASPs will be required to establish an international management system to promptly address customer complaints and enforce measures to resolve any disputes.

D. AML AND CFT

Similar to traditional financial intermediaries, the CASPs are required to fulfill customer due diligence requirements and have in place policies and procedures to detect, prevent, report illegal transaction.

- FATF – the Travel Rule

In 2019, FATF, an international body focused on combating money laundering and terrorist financing, introduced the initial global standard for AML/CTF. FATF member countries are now starting to integrate FATF Recommendation 16 into their individual AML regulations.[46]

When a CASP transfers crypto assets to a customer of another CASP, it is required to inform the receiving CASP of the identification information, including the name and blockchain address, of both the sender and the receiver ("Travel Rule").[47] The FATF recommends that countries adopt a minimum threshold of USD 1,000 for crypto-asset transfers. The transaction that exceeds the threshold shall identify the origins and destinations.

---

[42] Japan's PSA, 2019, Article 63-10, 63-11 and 64-12.
[43] Kanda Hideki, "Report from Study Group on the Virtual Currency Exchange Services" (FSA, December 2018) https://www.iosco.org/library/ico-statements/Japan%20-%20FSA%20-%2020181221%20-%20Report%20of%20the%20Study%20Group%20on%20Virtual%20Currencies.pdf, p.8.
[44] Claire Huang, "What Crypto Consumer Protection Rules Are There in the World?," The Straits Times, July 21, 2023, https://www.straitstimes.com/business/what-crypto-consumer-protection-rules-are-there-in-the-world.
[45] Kanda Hideki, "Report from Study Group on the Virtual Currency Exchange Services" (FSA, December 2018) https://www.iosco.org/library/ico-statements/Japan%20-%20FSA%20-%2020181221%20-%20Report%20of%20the%20Study%20Group%20on%20Virtual%20Currencies.pdf,p.6
[46] Tony Petrov, "Travel Rule 2023 - FATF Requirements for Crypto | the Sumsuber," Sumsub, March 28, 2024, https://sumsub.com/blog/what-is-the-fatf-travel-rule/.
[47] Gabija Stankevičiūtė, "What Is the Crypto Travel Rule? An Overview," iDenfy, April 22, 2024, https://www.idenfy.com/blog/crypto-travel-rule/#:~:text=The%20Crypto%20Travel%20Rule%20mandates.

- MAS - AML/CFT measures

Singapore's AML/CTF risk management standards are described in Notice PSN02 and apply directly to CASPs that fall under the PSA's scope.[48]

Notice PSN02 imposes CDD protocols, which are intended to prevent customers from opening anonymous accounts or managing accounts.[49] This identification requirement includes the collection of the customer's full name, identification number, residential address, etc.[50] When an exchange has reasonable notice grounds for believing that a particular account is being, or will be, used for illegal activity, it is prohibited from transacting with the customer or, if an existing business relation exists, it must report the account to MAS.[51] Additionally, the Notice PSN02 requires continuous risk assessment and mitigation measures.[52]

Moreover, CASPs are obligated to identify and assess the money laundering and terrorist financing risks that may arise concerning the development of new products and undertake risk assessments before the launch of such products.[53]

- Recommendations

It is essential for there to be clear international AML/CFT standards that are consistently applied across jurisdictions to address the money laundering and terrorist financing risks. The Regulator can follow FATF Recommendations by assigning greater responsibility and liability to CASPs to detect and actively report suspicious activities. In general, the AML/CFT measures to be imposed are similar to existing AML/CFT requirements (e.g., Know-Your-Customer -to record and verify the identity of customers, CDD, monitor transaction and suspicious transaction reporting) on other regulated entities. Following that, Regulator can set specific guidance for CASPs on identifying and reporting suspicious cryptocurrency transactions and set the amounts of monetary threshold to report.

As part of the risk assessment, Regulator needs to provide additional guidance for licensees to assess the risk posed by their new products. These products may have features that promote anonymity, obscure transactions, or hinder CASPs' ability to identify their customers. It is crucial to determine whether these products are known to be utilized by criminals for illicit purposes.[54]

IV. CONCLUSION

In conclusion, regulations for cryptocurrencies have been established in numerous jurisdictions, some of which are highly developed. Despite differences, each jurisdiction maintains distinct perspectives and considerations regarding cryptocurrency regulation.

The complex and comprehensive cryptocurrency regulatory landscape will present significant challenges for stakeholders in Cambodia. Unlike traditional financial institutions, the absence of a centralized counterparty makes it difficult to regulate crypto platforms consistently. While convergence is expected over time, the expectation of conventional institutional standards from relatively inexperienced CASPs underscores the need to address many issues. However, Regulator can gradually offer practical guidance and support to industry players. Overall, Cambodia still needs to consider several factors; recognizing the advantages of cryptocurrencies may prompt the RGC to reconsider its stance on allowing their use.

[48] MAS, Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism, 2 April 2024.
[49] Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism, 6.
[50] Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism, 6.6.
[51] Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism, 6.2 & 16.
[52] Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism, 6.25
[53] Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism, 5.
[54] MAS, "Frequently asked questions (FAQs) on the Payment Services Acts" (March 2022) https://www.mas.gov.sg/-/media/MAS-Media-Library/regulation/faqs/PD/faqs-on-payment-services-act-2019/Payment-Services-Act-FAQ--7-March-2022.pdf, p.17.

Deputy Prime Minister Aun Pornmoniroth, the Minister of Economy and Finance (center), and Dr Chea Serey, Governor of the National Bank of Cambodia.
Source: Khmer Times

THE PREVENTION AND PROTECTION AGAINST DIGITAL FINANCIAL TRANSACTION FRAUD IN CAMBODIA'S BANKING SECTOR

SOUN Somanut
is a PhD Candidate at the Royal Academy of Cambodia, specializing in the legal field with a focus on corporate, finance, and digital law. Throughout her career as a legal associate, she has gained extensive experience in various legal domains, particularly in commercial dispute resolution. Currently, she is conducting her PhD research on the effectiveness of the Cambodian legal framework in attracting foreign investment, with a specific emphasis on capital investment flows and the security of bank transactions.

I. INTRODUCTION

As the global economic landscape is moving toward digitalization, it leads Cambodia to witness a significant increase in terms of digital financial transactions practicing[1], with a report that approximately USD 492 billion in digital money had transferred to each other in 2023.[2] The engagement between consumers and merchants across the country is achieved by embracing the QR payment method.[3] This trend has made people feel more comfortable with cashless transactions and familiar with adopting e-commerce and e-government. It is even seen practiced in physical shopping, where smartphones are increasingly used instead of cash at checkout counters in supermarkets or with small vendors along the streets.[4]

While technologies bring a convenient transaction experience, there are also drawbacks from such development, commonly the "online fraud" in the banking system due to the rapid introduction of technology before the digital laws were in place to safeguard the security of people's practice in cyberspace strictly.[5] Not to mention, the International Criminal Police Organization (Interpol) has stated that in 2021, there were 7,345 cases of data theft reported to be conducted in Cambodia, and its primary target was from the banking sector, precisely 21.3 percent of it were from phishing attacks in the same year.[6]

Meanwhile, cybersecurity legislation to address specific issues is still lacking in Cambodia.[7] The existing regulations established by the National Bank of Cambodia (the "NBC") have served as the prudential regulatory framework to oversee and strengthen the proper practice and the security mechanisms of digital payment transactions.[8]

Since the Cambodian government still needs more years to adopt and implement the digital laws, legal issues arise regarding whether the prudential regulatory measures currently implemented by NBC have effectively ensured the safety of cyber problems in the financial sector. Such prudential regulatory measures include laws, prakas, regulations, and circulars ("legal framework") supervised by NBC.

This study will begin by examining Cambodia's existing financial law practices to analyze two key aspects: (1) the effectiveness of regulatory measures enacted by the NBC, which aims to mitigate potential financial cybercrime risks, and (2) the investigation of loopholes that could passively raise legal challenges within the ongoing context. Through this analysis, the research will likely provide comprehensive insight into the current cybersecurity landscape of financial institutions in Cambodia, hoping that the recommendations could contribute to developing cyberfinancial-related policies shortly.

II. NAVIGATING THE LANDSCAPE OF CYBERSECURITY PRACTICING IN CAMBODIA'S BANKING SYSTEM

"Cybersecurity" refers to the practice people conduct to prevent or respond to protect their information technology (IT) systems. This practice includes precaution procedures in infrastructure networks, operating systems, and computing programs against all forms of invasion and attacks from hackers over the internet.[9] On the other hand, "Prudential Regulations" focus on the legal policies aimed at securing

[1] Vichana Sar, "Opinion: Prioritize Bakong and Digital Banking for Financial Evolution," Cambodia Investment Review, April 2024, https://cambodiainvestmentreview.com/2024/03/20/opinion-prioritize-bakong-and-digital-banking-for-financial-evolution/.
[2] N.A, "Cambodia's Digital Transaction Volume Exceeds $492 Billion in 2023, Indicating Substantial Growth in Cashless Transactions," Cambodia Investment Review, April 2024, https://cambodiainvestmentreview.com/2024/04/01/cambodias-digital-transaction-volume-exceeds-492-billion-in-2023-indicating-substantial-growth-in-cashless-transactions/.
[3] N.A, "The Landscape of Digital Banking in Cambodia", Mad, accessed date April 2024, https://www.mad.co/en/insights/the-landscape-of-digital-banking-in-cambodia.
[4] N.A, "The Landscape of Digital Banking in Cambodia", op.cit.
[5] Nhean Chamrong, "NBC calls for strengthening cybersecurity across banks, financial institutions", Khmer Times, June 6, 2023, https://www.khmertimeskh.com/501302668/nbc-calls-for-strengthening-cybersecurity-across-banks-financial-institutions/.
[6] Nhean Chamrong, "NBC calls for strengthening cybersecurity across banks, financial institutions", op.cit.
[7] Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, Digital Economy and Business Committee, July 2023, p.ix.
[8] Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, p.5.
[9] Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, p.39.

the stability of financial institutions and financial systems.[10] Therefore, to discuss the legal frameworks aimed at preventing and protecting against digital financial transaction fraud in Cambodia's banking sector, it must involve overseeing the effectiveness of the prudential regulations supervised by NBC in the area of safeguarding the practice of customer and the financial institution in how they are using the technology to manage their financial transactions.

To ensure cybersecurity risk in the banking system, data privacy is reported as a significant concern.[11] The government of Cambodia believes that cybersecurity and data protection are linked and must be considered together as wings required for the development of the digital sector.[12] To simplify, ensuring cybersecurity does require action to protect users' data and protect user data, the private sector must comply with the cybersecurity standards.[13] Therefore, the Royal Government of Cambodia has prioritized strategic plans to build and strengthen FinTech, which is the tree of various areas in the digital financial system, including digital payment.[14] So far, there is a notable achievement in the implementation of KHQR, which features an "Easy to Scan – No Confusion" function.[15]

Considering the ongoing development of Fintech in the concurrent digital laws drafting era, including but not limited to the development process of the cybersecurity laws and data protection laws, it appears that currently, high-level governance is absent responsible for cyber issues in Fintech; hence, the NBC has become the sole competent regulator that holds power to instruct, circulate, regulate, or decided on all matter related to Fintech with the support from other ministries/institution as requested by the NBC,[16] which make the NBC has now served as the governance body that all Critical Information Infrastructure (CII) operators, such as banks, shall rely on.[17]

III. THE REGULATORY MEASURES TO ADDRESS PERSONAL DATA SECURITY IN BANKING CYBER ATTACKS

In the capacity of a sole competent authority that oversees all issues arising in the banking system of Cambodia, so far, the NBC has adopted numerous legal frameworks aimed at shaping a safe and friendly environment for financial transactions, including parkas that carry the purposes to secure the personal data of all bank users.[18]

Let's draw attention to when the bank user wishes to open a bank account under the legal requirements, certain personal information such as the account owner's full name, date of birth, identity card/passport number/identity document reference number, occupation/business, address, and nationality[19] is required to submit to the bank as advised by Prakas on Anti-Money Laundering and Combating Financial Terrorism ("AML/CFT"). In addition, the bank shall have a strict responsibility to safeguard its customers' sensitive personal data, which affects customers's financial and personally identifiable information, while having its role as the CII.[20] This is considered an essential task since personal data is sensitive and plays a significant role in the transfer process.[21] Under the supervision of NBC, the non-compliance CII shall result in disciplinary sanction if it fails to protect the customer information.[22]

[10] Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, p.40.
[11] Andrew P. Scott, Paul Tierno, Banking, Data Privacy, and Cybersecurity Regulation, (Congress Research Service, March 13, 2023), summary.
[12] Royal Government of Cambodia, Cambodia Digital Economy and Society Policy Framework 2021-2035, The Supreme National Economic Council, May 2021, p.16.
[13] Royal Government of Cambodia, Cambodia Digital Economy, p.16.
[14] Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, p. 9-10.
[15] Leng Sereywath, Bakong as a payment switch, National Bank of Cambodia, November 2020, p.2.
[16] Law on the Organization and Conduct of the National Bank of Cambodia, Article 33.
[17] Law on Banking and Financial Institution, Article 6.
[18] Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, p.5.
[19] Prakas on Anti-Money Laundering and Combating Financial Terrorism, Article 6.
[20] Law on Banking and Financial Institution, Article 51.
[21] Law on Anti-Money Laundry and Combating Financial Terrorism, Article 16.
[22] Law on Banking and Financial Institution, Article 41.

1. THE IMPLEMENTATION OF KHQR ENCRYPTION TO PREVENT DATA EXPOSURE AND FRAUDULENT MONEY TRANSFERS

The KHMER QUICK RESPONSE CODE ("KHQR") is a successful FinTech product of the NBC, which was established and introduced to the public as a specification code in Cambodia through Prakas no. B14-020-351 on 26 June 2020. Its primary aim is to create a more convenient environment for digital financial transactions and, at the same time, strengthen data security standards.[23] The application works by encrypting information into a standard code that could offer quick access to the digital money transformers via scanning through that encrypted QR code. With this establishment, KHQR prevents both data exposure and fraudulent activities, such as transferring money in the wrong amount and to the wrong account.[24]

Encryption means converting data into a coding format.[25] In each financial transaction, the receivers were previously required to share their bank account and name if they wanted the other party to transfer money to their bank accounts. However, following this KHQR design, the receiver's data is organized in a tree-like structure of data objects,[26] with the benefit of protecting private information like bank account numbers and the receiver's full name. As a result, the KHQR has prevented exposure to data information and help in ensuring people's identity in cyberspace.

Another safety condition that the digital money receiver could benefit from such technology is the accuracy of the payment. With encryption, the receiver can set up the payment amount and encrypt it with a specific code, ensuring the funds are transferred in the correct amount and to the proper account.[27] Before KHQR, there was no particular procedure for solving fraudulent issues associated with the specific payment amount. In previous practice, when a dispute about digital transactions appeared, it was noticed in existing law that NBC could provide a resolution platform that merely focused on issues like delayed transactions or lack of clear information.[28] Fraudulent activities, such as transferring an incorrect amount of money to the proper account number, were beyond the scope of NBC's capacity since this aspect typically involves private interactions between parties. As a result of KHQR, this problem will be eased.

Overall, KHQR's initiative provides a simple, fast, and secure payment method and aims to mitigate fraud by eliminating the need to share account numbers, thus increasing security in the face of common hacking threats. It is also stated in the governmental policy of Cambodia that to safeguard the development of financial technology, relying on the relevant laws and regulations alone is not enough; the development of digital infrastructure significantly contributes to safe innovation and encouragement of the use of digital payments.[29] According to Prakas no. B14-020-351, NBC has urged all banks nationwide to adopt KHQR as a mandatory standard no later than 2020. Those who fail to comply will receive a penalty.[30]

2. SHIELDING AGAINST FINANCIAL CRIMES IN PROTECTING AGAINST IDENTITY THEFT IN BANKING

Meanwhile, the critical discussion of identity theft in the banking system may be about phishing scams or unauthorized fund transfers. Article 7 of the AML/CFT Law clearly states that all bank accounts opened by banks must have their personal information recorded, and they must prevent the opening of accounts for anonymous individuals. Even though cases of faking bank accounts have not been reported in Cambodia before, it is noteworthy that this procedure is a highly effective preventative regulation that the government of Cambodia has implemented. Indeed, the information provided by the Anti-Cybercrime Department indicates that Cambodia has experienced cases where identity theft has occurred through

[23] Prakas on Introduction of KHQR Technical Dating Template for Payment, Article 2.
[24] Prakas on Introduction of KHQR Technical Dating Template for Payment, Annex, Dynanic QR Code, p5.
[25] Prakas on Introduction of KHQR Technical Dating Template for Payment, Annex, QR Code Payload Data Objects, p5.
[26] Prakas on Introduction of KHQR Technical Dating Template for Payment, Annex, p2.
[27] Prakas on Introdiction of KHQR Technical Dating Template fpr Payment, Annex, Dynanic QR Code, p5.
[28] Prakas on Resolution on Consumer Complaint, Annex.
[29] Royal Government of Cambodia, Cambodia Financial Technology Development Policy 2023-2028, p6.
[30] Prakas no. B14-020-352, Article 5.

social media platforms, in which the fraudster has faked the identity to scam for financial benefit from other social media users.[31] Therefore, if bank accounts are easily opened without stringent personal data screening, this will create the possible channel that leads to identity theft in the banking system, facilitating severe crimes like money laundering, ransomware attacks, or illegal loan sharking.

Under Article 3.1 of the AML/CFT Law, "Money Laundering" refers to the conversion or transfer of property in a way that the transferer does not justify the illicit origin of the property, which also includes the true nature of the funds. Even if the AML/CFT Law does not explicitly address the issue regarding transactions involving online fraud, however, as stipulated in Articles 5.1 and 5.3 of the Prakas on AML/CFT, it provides a proper environment to urge bank institutions to verify and identify the data or information regarding customer due diligence, which can help prevent activities involving criminals creating bank accounts using stolen personal identities to shift legal liabilities to someone else, and then using these accounts to receive illicit funds from criminal activities, including but not limited to drug trafficking or fraud from ransomware attacks.

IV. EXERCISING LEGAL FRONTIERS OF CYBERSECURITY CHALLENGES IN CAMBODIA

After navigating digital financial transactions in Cambodia, the legal framework to address cybersecurity responsibility in online fraud remains comprehensive. At the same time, regulations from the NBC aim to guide financial institutions in working systematically in the economic aspect, but none directly tackle cyber-attacks or cyber fraud.

NBC is not to blame for this issue. NBC originally functioned in the financial sector. Hence, in the era of technology integration, NBC requires time and support from other technical teams in Cambodia to develop a strategy and hybrid legal framework that could raise the standard of legal understanding of finance and technology. This is a collaborative effort that cannot be undertaken alone. It requires joint participation in several vital aspects.

1. THE SELECTION OF LEGAL SYSTEM APPROACH: FULLY FLEDGE CYBERSECURITY LAW VS. STATUTORY ACTS

In a situation where the law governing data privacy has not been established and is still in the process of drafting, Cambodia is using its general principle to deal with any form of attack in cyberspace temporarily. Those are the legal procedures that are forth under the tree of Cambodia's core legal framework, such as the Constitution, the Civil Code, and the Criminal Code, and they follow the specific law that is lying under each area of practice.[32] For instance, the legal framework supervised by NBC will be discussed in this FinTech-related issue.

Based on a study from the World Bank on cybersecurity in the financial sector, countries globally have adopted two types of cybersecurity law approaches: "a fully-fledged" and "a statutory act."

A fully-fledged is a comprehensive approach that a country chooses to promulgate cyberlaw as the core principle, then establish a specific working group as a competent authority to apply the theory or handle its implementation in different areas. This practice is seen in countries like China and Singapore.[33] For instance, by relying on the Singapore Cyber Security Act No.9 of 2018, the Commissioner of Cybersecurity serves as the main body of the country to address cybersecurity issues, including investigation, impact assessment, and conducting procedures to prevent and respond to further harm.[34]

[31] Anit-Cyber Crim Department, the Social Media Scam, April 9, 2024, https://www.facebook.com/photo/?fbid=815987903894575&set=a.302286868598017.
[32] Phin Sovath, Law in the Digital Age: Protection of Consumer Rights, Konrad Adenauer Stiftung, 2021, p.51.
[33] Legal Framework for Cybersecurity in the Financial Sector: A Comparative Study on Existing Domestic or Regional Legislation on Cybersecurity, World Bank Group, February 2022, p.1.
[34] CAS Singapore, Cybersecurity Act, https://www.csa.gov.sg/legislation/Cybersecurity-Act#:~:text=The%20Act%20empowers%20the%20Commissioner,or%20cybersecurity%20incidents%20from%20arising.

Another aspect involves adopting "statutory acts," which are adopted in many key areas to cover different specific matters instead of relying on a single Cyberlaw.[35] This practice is seen in the United States, where other acts cover various issues such as information sharing, data breaches, or consumer privacy protection.[36]

Hence, while looking forward to successfully establishing a legal framework related to FinTech, identifying a transparent approach to its specific legal system is also an asset to fastening the development.

2. THE DEFINITION OF RESPONSIBILITIES AND GROSS NEGLIGENCE IN CYBERSECURITY LAW

Along with the legal drafting process, it is proposed that Cambodia has clear legal definitions to mitigate fraud and ensure data protection. To serve this goal, it involved the clear interpretation of two key terms: "the responsibilities" of financial institutions and bank users and what can be defined as "negligence" of the parties to comply with cyberlaw. Negligence must be clearly defined from non-awareness.

Once digital financial fraud incidents arise, NBC generally collaborates with the Ministry of Interior to apprehend fraudsters. However, there is no established procedure to determine who is responsible for financial losses, whether the bank can help the customer recover the lost money, or whether the bank should bear the responsibility.

Regarding the practice of member countries of the Basel Committee on Banking Supervision, those countries have successfully designed clear jurisdictions for handling responsibilities and gross negligence. Clear legal definitions ensure that both banks and customers understand their roles. These countries typically require banks to bear the loss from fraudulent activities, ensuring their citizens are protected. However, an exception is made in cases of fraudulent or grossly negligent behavior by the user.[37]

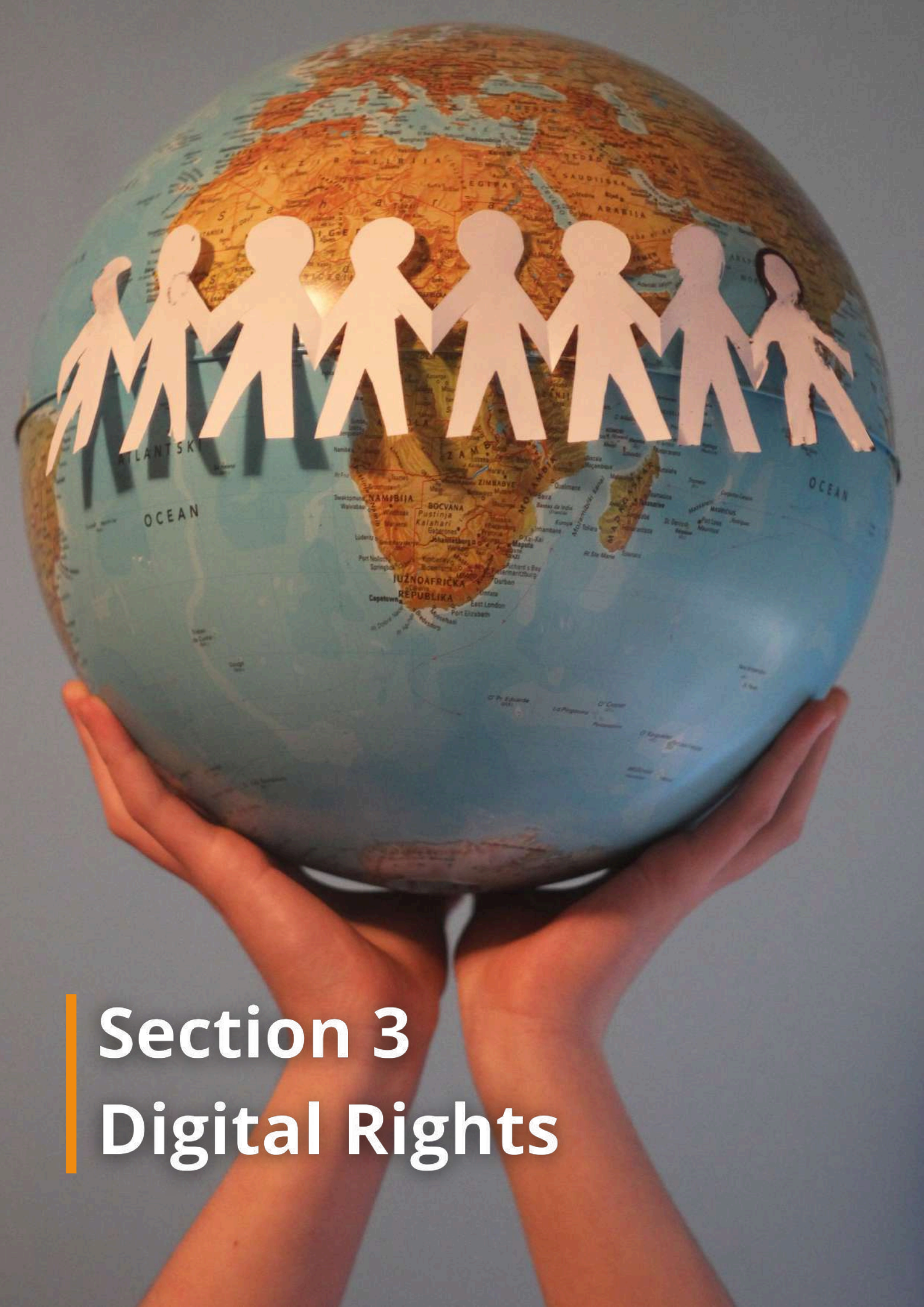
V. CONCLUSION

To conclude the studies, we have examined that the rapid advancement of FinTech has brought convenient digital transactions to Cambodian citizens of all ages, and at the same time, such technological development has also introduced cybersecurity threats that could trigger bank users to embrace significant financial losses at any minute. Therefore, the regulatory framework shall be addressed promptly in response to such development; meanwhile, the adoption of digital laws is still pending, which leads to the primary responsibility falling primarily on financial regulation to govern technological developments in the banking system.

While NBC has implemented regulations and procedures to safeguard online transactions and mitigate potential cybercrime risks, these measures do not comprehensively address the issue of digital fraud. Although cooperation from the user is the most critical factor in preventing some risks, the regulator shall play a role in eliminating incidents against unforeseen misfortunes. Therefore, the forthcoming adoption of Cybersecurity and Data Protection laws is vital as a robust supportive measure and needs to be in place as soon as possible to substitute the current legal framework that is still leaving a loophole in dealing with cyber criminals.

The current journey of Cambodia's financial digital landscape might embrace some cybersecurity challenges; however, relying on the upcoming governmental plan of Cambodia, along with the successful adoption of the Cybersecurity Law and Personal Data Protection Law of Cambodia, it is believed that Cambodia is walking through a healthy environment of digitalization.

[35] Legal Framework for Cybersecurity in the Financial Sector, p.1.
[36] A Glance at the United States Cyber Security Laws, appknox, accessed April 2024, https://www.appknox.com/blog/united-states-cyber-security-laws.
[37] Digital fraud and banking: supervisory and financial stability implications, Basel Committee on Banking Supervision, February 16, 2024, p 6-8.



Section 3
Digital Rights

Source: ACLU

NAVIGATING THE DIGITAL FRONTIER: UNPACKING THE INFLUENCE OF ARTICLE 97 OF THE LAW ON TELECOMMUNICATIONS ON PRIVACY AND JUSTICE

NELSON Elan

is a law graduate student. He has recently earned two Bachelor's in Law, from the American University of Phnom Penh (AUPP) and the University of Arizona (UA) respectively. Apart from academics, he participated in the 2023 Jessup Moot Court Competition and the 2023 Asia-Pacific National Moot Court Competition. In addition to being one of the KASFLY 2024 fellows, he currently works as a library assistant at AUPP. His primary legal interests are in Copyright law and Human Rights law.

I. UNVEILING THE JOURNEY: AN INTRODUCTION

The following brief will examine the intricate contrast between how rights in the digital space and the physical world are implemented. This contrast will be analyzed by focusing on the implications of Article 97 of the Law on Telecommunications in Cambodia on the rights to privacy and fair trial. The discussion on digital human rights has been around for a while and continues to be a contentious topic as technology advances. At the center of this discussion is the issue of how human rights can and should be implemented in digital spaces.

This brief will contribute to this discussion by criticizing Article 97's alignment with international standards, focusing on the International Covenant on Civil and Political Rights (ICCPR), and then comparing its effectiveness with the United States, Singapore, and European Union jurisdictions. Communications Decency Act (CDA) Section 230 and the Foreign Intelligence Surveillance Act (FISA) Section 702 will be discussed for the US. For Singapore, Sections 24 and 26 of the Personal Data Protection Act (PDPA), along with Sections 8A and 8B of the Computer Misuse and Cybersecurity Act (CMCA). Lastly, Digital Services Act Articles 24, 25, and 26, in addition to Article 5(a), Article 6(1)(a) and 6(1)(b) for the EU. Also, it will analyze the legal nuances concerning infringement on fundamental human rights. The main legal issue of this brief lies in Article 97's vague terminology and broad applications. Article 97 is of concern because of its potential violation of Articles 14 and 17 of the ICCPR.

This is due to the provision lacking clarification on the term "legitimate authority", broad application regarding what is a "legitimate authority," and the possible infringement on the right to privacy. The degree of balancing government interest in national security with individual digital rights will also be analyzed and questioned. This brief addresses these legal challenges by answering the following research questions:

1. To what extent does Article 97 of the Law on Telecommunications infringe on digital human rights, especially Articles 14 and 17 of the ICCPR?
2. How does this legal provision compare to the international standard and similar provisions in other jurisdictions in terms of protecting digital human rights, namely the United States, European Union, and Singapore?

II. NAVIGATING THE GLOBAL LANDSCAPE OF DIGITAL HUMAN RIGHTS

Before Article 97's adherence to international standards can be evaluated, the international standard must be established first, followed by whether the Cambodian Constitution is in line with that standard[1]. For Cambodia, Article 40 of the Cambodia Constitution primarily enshrined the right to privacy. So, the following sections will establish the international standard for digital human rights and the extent to which the Constitution has a legal obligation to abide by that standard.

1. THE INTERNATIONAL STANDARD: A NEW FRONTIER

The United Nations (UN) views digital human rights as equivalent to traditional human rights, emphasizing their protection both online and offline.[2] Therefore, these rights should be protected in a similar manner to human rights, with the added recognition of the differing boundaries between the physical and digital space.[3] Legal provisions governing digital human rights stem from International Human Rights Law, particularly the ICCPR.[4] Article 17 of the ICCPR specifically addresses the right to privacy and "protects individuals from arbitrary interference with that right". The right to privacy involves protection from interference with an individual's home, family, communications, and unlawful surveillance, including the

[1] Constitution of the Kingdom of Cambodia, Article 40 (1993).
[2] UN Human Rights. n.d. The Impact of Digital Technologies on Human Rights. United Nations. Digital space and human rights | OHCHR
[3] Shany, Yuval. Digital Rights and the Outer Limits of International Human Rights Law. German Law Journal 24, no. 3 (2023): 461–72. https://doi.org/10.1017/glj.2023.35.
[4] UN General Assembly. International Covenant on Civil and Political Rights, United Nations, Treaty Series, vol. 999, p. 171, 16 December 1966, Article 14 & 17. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

usage of listening devices. The broad application of Article 17 indicates anticipation for privacy rights protection to become more complicated over time as protection is no longer limited to the physical world.

2. THE CAMBODIA CONSTITUTION: A LOCAL PERSPECTIVE

According to Chapter III, Article 31, and Article 32 of the Cambodian Constitution, the Cambodian Constitution recognizes the UN Charter along with all covenants and conventions related to human rights. Article 31 is, therefore, evidence of Cambodia's adherence to the legal stance established by the UN since it recognizes the UN Charter. This recognition indicates a legal commitment that supports the UN's stance regarding digital human rights. Thus, the Cambodian Constitution is in line with the international standard.

III. A CRITICAL EXAMINATION OF ARTICLE 97

It is crucial to analyze the key language in Article 97 to examine whether it violates the digital human right to privacy. This section provides definitions for the key terminology in Article 97 and analyzes its potentially broad application.

1. UNPACKING 'LEGITIMATE AUTHORITY'

The term "legitimate authority" refers to "power whose use is considered to be appropriate and just by those for whom that power is exercised".[5] Furthermore, the term "legitimacy" refers to the fact of being allowed by law or done according to the rules of an organization or activity.[6] In Article 97, "legitimate authority" is not clearly defined, which can lead to digital human rights violations. Violations inevitably arise from the misuse of digital technology to infringe on such rights through unlawful surveillance, censorship, or discrimination.[7] ICCPR Article 14 holds that every individual has "the right to a fair and public hearing by a competent, independent, and impartial tribunal established by law". Article 17 protects individuals from "arbitrary or unlawful interference with their privacy, including family, home, and correspondence". The lack of clarity on the definition of a legitimate authority may allow for the misuse of surveillance powers, leading to violations of confidentiality of communications and due process rights. Article 97 is at risk of not being compliant due to this ambiguity for those provisions of the ICCPR.

2. DEFINING BOUNDARIES

A sub-decree that defines which institutions are designated "legitimate authorities" should be enacted to mitigate privacy violations since the term is too broad. This would provide a clear framework and prevent potential abuse through the usage of the term. Doing so would then provide more protection to the privacy rights of individuals, as they can be assured that there is a structure in place to mitigate violations of their privacy. This action would then further the recognition of digital human rights as the concept emphasizes the necessity for clarity in how laws, such as the aforementioned Article 97, are applied in the digital space.

IV. A COMPARATIVE ANALYSIS OF LEGISLATION IN THE EU, SINGAPORE, AND THE US

1. THE UNITED STATES: A CLOSER LOOK

In the United States, the intersection of digital technology and human rights has become a contentious point of discussion, specifically found in Section 230 of the Communications Decency Act (CDA)[8] in addition to Section 702 of the Foreign Intelligence Surveillance Act (FISA).[9] These laws give platform

[5] Weber, M. (1978). Economy and society: An outline of interpretive sociology (G. Roth & C. Wittich, Eds.). Berkeley: University of California Press. (Original work published 1921)
[6] 'Meaning of Legitimacy in English'. Cambridge Advanced Learner's Dictionary & Thesaurus. Cambridge University Press. Accessed March 7 2024. https://dictionary.cambridge.org/dictionary/english/legitimacy
[7] 'Digital Space and Human Rights.' United Nations Human Rights Office of the High Commissioner. Accessed March 14 2024. https://www.ohchr.org/en/topic/digital-space-and-human-rights
[8] Communications Decency Act, Section 230(1), February 8, 1996 , 104–104, 110 Stat. 137, Pub. L. 105–277, div. C, title XIV, § 1404(a), Oct. 21, 1998; Pub. L. 115–164, § 4(a), Apr. 11, 2018.
[9] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Section702. Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons, 110–2614. July 10, 2008. 50 U.S.C. § 1881a

owners liability protections for content posted by their users, regulation for the removal of harmful content, and set legal boundaries for U.S. intelligence agencies for foreign intelligence gathering.

2. BALANCING FREEDOM AND RESPONSIBILITY

Section 230 of the CDA provides a liability shield to online platforms for content their users post. Section 230(1) gives Publisher Immunity, which protects online platforms from liability for content posted by users through not treating them as the publisher and speaker of that content. But only if that content is from another provider, such as a user. Section 230 also does not impose a duty to monitor for offensive content. This legislation has been criticized for allowing online platforms to essentially shed responsibility for moderating harmful content. However, it has also been argued that this law is necessary for protecting freedom of speech online. It allows users to freely express their opinions without online platforms needing to be restrictive to mitigate their liability.

3. NATIONAL SECURITY IN THE DIGITAL AGE

For the provision from FISA, Section 702 allows U.S. intelligence agencies to acquire foreign intelligence from foreign nationals "believed to be located" outside the U.S. The process requires the Attorney General (AG) and Director of National Intelligence (DNI) to submit certifications specifying what foreign intelligence is to be collected to the Foreign Intelligence Surveillance Court (FISC) for review. The FISC then analyzes the certifications for target information and the procedures in place to ensure compliance with the FISA Act and the Fourth Amendment on protecting privacy. After review, once given approval, the AG and DNI are then able to issue written directives to compel U.S. electronic service communication services providers to assist with collecting intelligence on the approved targets. The Department of Justice (DOJ) then reviews every target the AG and DNI determine before collecting intelligence. The oversight of this approval process indicates an effort to protect privacy rights while maintaining national security. A critique of this provision is that the approved intelligence gathering could also lead to warrantless searches of American citizens' communications when in contact with foreigners abroad. An example of this was the apprehension of Najibullah Zazi, who resided in the state of Colorado in the U.S. and was discovered by authorities to be in communication with al-Qaeda terrorists in Pakistan and conspired with them to bomb New York City in 2009. Intelligence gathering through Section 702 prevented this attack, but it involved the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) violating the communication privacy of an American citizen without a warrant.[10]

4. PIONEERING DIGITAL LEGISLATION

The EU's Digital Services Act (DSA)[11] and Digital Markets Act (DMA)[12] play an essential role through their respective aim to create a safe and predictable online environment for individuals and stakeholders alike. The following sections will analyze the legal frameworks in the EU that govern and protect digital privacy.

5. REDEFINING ONLINE SERVICES

DSA Articles 24, 25, and 26 address transparency in advertising, recommender systems, and data usage, respectively. Article 24 mandates transparency in online advertising. Article 25 requires that users be given an explanation of the main parameters for recommender systems and offers them influence over those parameters. Article 26 obligates platforms to provide clear information on what data is collected and processed. These provisions protect individuals' privacy by informing them of how their data is used and giving them a degree of control over their data.

[10] National Security Agency. (n.d.). The Foreign Intelligence Surveillance Act of 1978 (FISA) Overview. Retrieved from: https://www.nsa.gov/Signals-Intelligence/FISA/

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) Article 24, 25 & 26. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[12] 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 and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) Article 5(a) & Article 6(1)(a)(b). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925

6. REGULATING THE DIGITAL ECONOMY

DMA Article 5(a) prohibits the combining of personal data without consent, with Articles 6(1)(a) and 6(1)(b) addressing data portability and interoperability. Article 5(a) prohibits gatekeepers from combining personal data without user consent. Article 6(1)(a) ensures data portability for users, with 6(1)(b) requiring interoperability of instant messaging services.

Article 5 as a whole has been critiqued by Moreno Bellos and Petit, who pose that the DMA's ambiguous nature creates challenges for practical implementation. This is evident in the lack of scope of obligation for a "gatekeeper" in the context of Article 5(a), which makes the provision difficult to enforce and company compliance a challenge. Furthermore, there is concern that the evolution from the GDPR to the DMA has created gaps in the regulation of entities such as tech companies as data management continues to become more complex.[13] In addition, the interoperability requirements are also challenging to implement as the technical standards are not clear in 6(1)(b), which potentially hinders the development of compliant interoperable systems.[14]

7. SINGAPORE: A CASE STUDY IN CYBERSECURITY

Singapore has taken significant strides to ensure privacy protection. The country's legal framework for digital privacy protection is primarily governed by two pieces of legislation: the Personal Data Protection Act and the Computer Misuse and Cybersecurity Act. These laws form the basis of the following sections, which will dive deeper into the state of digital privacy protection law in Singapore. The aim is to provide a comprehensive understanding of the present landscape and discuss potential areas of strength and criticism.

8. SAFEGUARDING PRIVACY

The Personal Data Protection Act (PDPA) is Singapore's cornerstone of data protection. It requires personal data to be protected and individual consent to be sought before it can be used.[15] Section 24 emphasizes the necessity of security for preventing unauthorized data access, and Section 26 requires explicit consent for data collection and usage. The Act also holds exemption clauses criticized for being broad and weakening the protection provided to data under Section 4. Wong Yong Quan, in the International Data Privacy Law Journal, highlighted how those exemptions can potentially undermine data privacy.[16]

9. DEFENDING AGAINST CYBER THREATS

The Computer Misuse and Cybersecurity Act (CMCA) criminalizes authorized data access. Section 8A addresses the retaining and supplying of personal data obtained through cybercrime, with Section 8B covering severe cyber crimes in Singapore. The concern about the CMCA is its focus on personal information and extraterritorial authority. Carr and Williams, in the International Journal of Law and Information Technology, argue that the provisions of the Act possibly disregard the human rights of suspected criminals and introduce questions over the necessity of having those provisions.[17] The Act also fails to address non-personal data misuse, such as trade secrets, which have been highlighted as a serious oversight by Norton Rose Fullbright's publication on Singapore Cybersecurity.[18]

---

[13] Pathak, Maitrayee, Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act. (6 February 2024). delivery.php (ssrn.com)
[14] Moskal, A. M. (2023). Digital Markets Act: A Consumer Protection Perspective. European Papers, 7(3), 1113-1119. https://www.europeanpapers.eu/en/system/files/pdf_version/EP_EF_2022_H_005_Anna_Moskal_00615.pdf
[15] Personal Data Protection Act, Section 4, Section 24 & Section 26, May 27, 2019. No. 136, Chapter 69. https://sso.agc.gov.sg/Act/PDPA2012
[16] Wong, B. Y. (2017). Data Privacy Law in Singapore: Personal Data Protection Act 2012. International Data Privacy Law, 7(4), 287-302. https://doi.org/10.1093/idpl/ipx016
[17] Carr, I. M., & Williams, K. S. (1998). A step too far in controlling computers? The Singapore Computer Misuse Act 1998 (Amendment). International Journal of Law and Information Technology, 8(1), 48-64. https://doi.org/10.1093/ijlit/8.1.48
[18] OneTrust Data Guidance & Rajah & Tann Asia. (2022) Comparing Privacy Laws: GDPR v. Singapore's PDPA https://www.dataguidance.com/sites/default/files/gdpr_v_singapore_2022_july_update.pdf

V. STRATEGIES FOR ENSURING COMPLIANCE: A ROADMAP

Cambodia could employ various solutions to address violations of digital human rights. An expert from the United Nations, Ana Brian Nougreres, presented three recommended approaches.[19] The first is the adoption of legal frameworks that provide remedies for the protection of violations of personal data protection. To affirm their right to privacy, individuals need a mechanism for seeking remedies when that right is breached. Second, identification and consideration for adopting privacy legislation from other countries that hold "stronger guarantees" for effectively realizing privacy rights in the digital space. Having a checks and balance system, as seen through FISA, would provide such guarantees. Finally, another solution would be making a clear list of institutions that are legitimate authorities, establishing criteria for an institution to qualify as a legitimate authority, or doing both to further transparency with the public.

Solution three provides the best outcome because a clear list of institutions would serve as a reference for Ministries and individuals themselves. Implementing this solution would ensure compliance with the ICCPR and strengthen the protection of individuals' right to privacy and fair trial by aligning with the principles of the ICCPR.

1. RECOGNIZING THE CHALLENGES

The aforementioned solutions still need to be revised. Cambodia's law regarding data protection is still in the womb of nations such as the U.S., which have decades of law that culminated in the FISA and CDA, respectively. However, the proposal to create a clear list of institutions recognized as legitimate authorities is promising. There is evidence of the success in minimizing rights violations, as seen with the FISC, despite the bureaucracy involved in obtaining certification approval.[20] Further, institutions such as the Ministries also possess a dynamic nature, and their role in the Cambodian legal system would require any criteria for an institution to qualify as a legitimate authority to be adaptable and flexible to changes.

While these solutions provide a robust approach to protecting digital human rights, they should be viewed as part of an ongoing process requiring constant evaluation and adaptation to serve Cambodia's needs better. It is crucial to ensure that these solutions do not infringe upon other rights or create new forms of exclusion or discrimination.

2. CHARTING THE PATH FORWARD

For now, there are two possible solutions. The first approach is amending Article 97 to clarify its terminology and narrow its scope of application. Another approach is implementing strict oversight and transparency measures when applying the law to ensure it is not misused. This solution could exist in the form of a specific overseeing Ministry or other institution with a certification and approval process to minimize digital human rights violations by authorities. In addition, the process would require authorities to report whose communications they are collecting, what purpose they are collecting it for, and what evidence they have that warrants the usage of Article 97.

3. IDENTIFYING THE SUPERIOR SOLUTION

The most effective solution would be a combination of the first and second approaches. Amending Article 97 to clarify the terms and scope of the application would address the root of the problem. However, strict oversight and transparency measures would strengthen public trust and ensure the law is fairly applied. Thus, this combined approach would address the problem's cause and symptom, making it the superior solution.

[19] Brian Nougeres, A. (2024). "Individuals must be able to realise the right to remedy for privacy violations in data protection". United Nations Human Rights Council. https://www.ohchr.org/en/press-releases/2024/03/individuals-must-be-able-realise-right-remedy-privacy-violations-data
[20] Liu, Edward C. "Foreign Intelligence Surveillance Act (FISA): An Overview." Congressional Research Service, April 11, 2024. https://crsreports.congress.gov/product/pdf/IF/IF11451

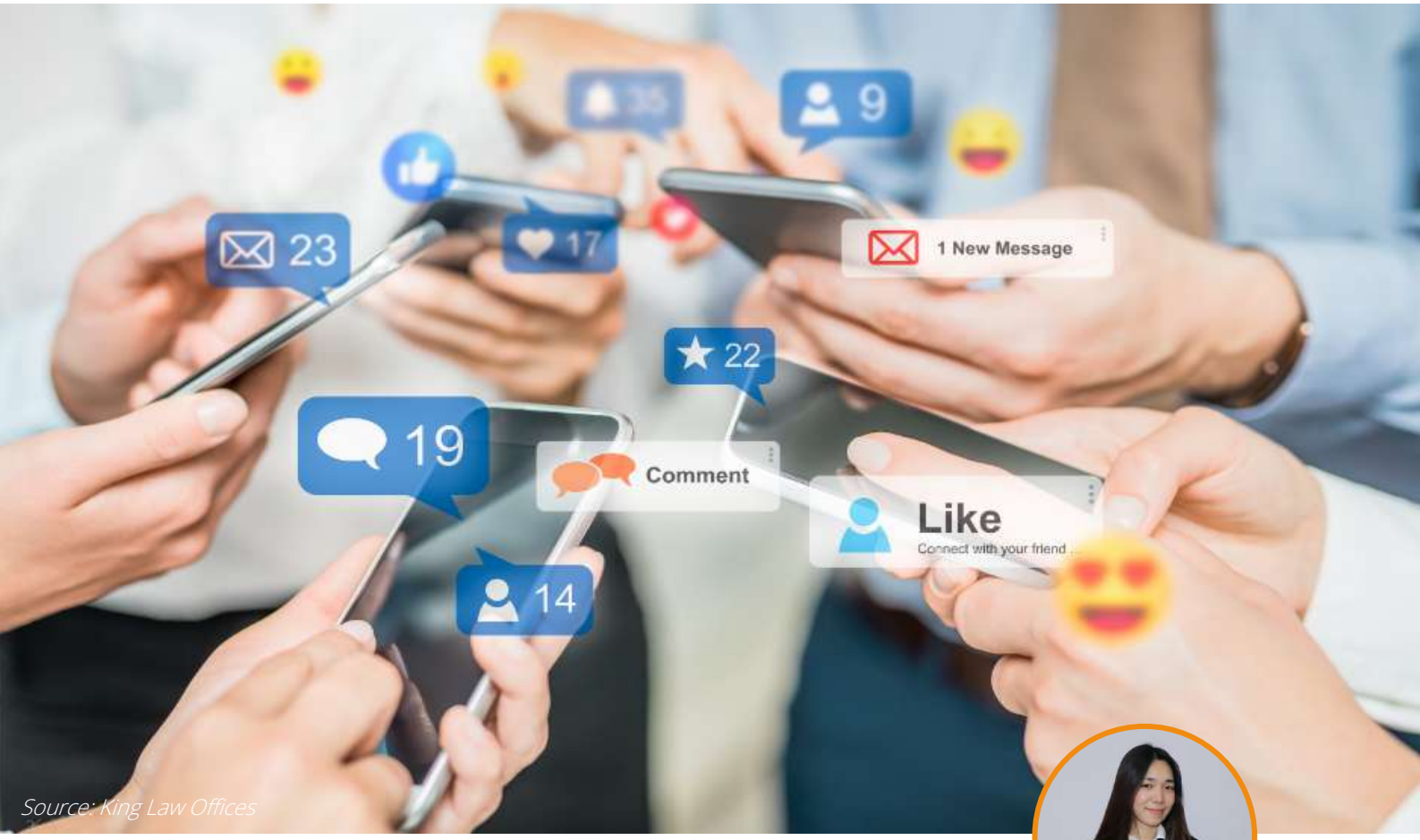
4. ACKNOWLEDGING THE OBSTACLES

This solution does have some limitations. Amending a law is a lengthy and complex process that also requires input from stakeholders affected by that law. While oversight and transparency measures could prevent misuse of the law, such measures require robust procedures to be effective. There is also the potential for resistance from those who benefit from the current ambiguity of Article 97. However, despite these challenges, the proposed solution offers the best chance of strengthening public trust while ensuring the law continues to serve its intended purpose.

VI. CONCLUSION: REFLECTING ON THE JOURNEY AND LOOKING AHEAD

To conclude, the core of this brief rests on the careful examination and interpretation of the law. The central argument, alongside the discussed discourse, underscores the need to harmonize Article 97 with international human rights law standards. The constraints of this brief must also be recognized. Despite extensive research, some aspects could have been discussed but still need to be addressed. These are not shortcomings but boundaries limited by the scope of this brief.

These constraints still pave the way for future exploration of the main issue explored. The solutions identified but not fully fleshed out could form the basis of future research. This could supplement the arguments made in this brief and position this contribution to encourage others to expand on and progress the law toward compliance with protecting digital human rights.



Source: King Law Offices

ESTABLISHING A LEGAL FRAMEWORK TO BALANCE BETWEEN FREEDOM OF EXPRESSION AND DEFAMATION IN THE DIGITAL AGE

KONG Kanary
is a senior student pursuing a dual degree in the English Language Based Bachelor of Law (ELBBL) at the Royal University of Law and Economics (RULE) and a Bachelor of English at the Institute of Foreign Languages (IFL). In her law school journey, besides being one of the KASFLY 2024 fellows, she has participated in the 2022 International Humanitarian Law (IHL) Moot Court Competition and 2023 Nuremberg Moot Court Competition. Nary has a keen interest in international criminal law, human rights law, and corporate law.

I. INTRODUCTION

Cambodia has undergone a notable transition into the digital era, characterized by a significant reliance on social media platforms for communication, information dissemination, and business transactions. This shift is evidenced by the increase of internet users by 714 thousand between 2022 and 2023, indicating the pervasive influence of digital technologies on Cambodian society.[1] However, with their significant benefits, social media platforms have also amplified the spread and impact of harmful content, including misinformation and defamation, by enabling rapid dissemination to a vast audience and creating echo chambers reinforcing false information. These issues represent a double-edged sword. On one hand, individuals may exploit freedom of speech protections to avoid legal consequences. On the other hand, defamation laws can sometimes threaten freedom of speech by penalizing individuals for expressing their opinions. For instance, the business owner may pursue a defamation claim against the customer if the customer's statement, though accurate, impacts the business owner's ongoing sales. Vice versa, the customer may use the freedom of speech just to spread false information to damage the business's reputation.

Addressing the expansion of misinformation on social platforms requires careful consideration to strike a just and operational balance between freedom of speech and anti-defamation recourse. Cambodia has laws governing these issues, including the Cambodia Criminal Code, Constitution Law, and Consumer Protection Law. In light of these challenges, this research paper aims to propose an adaptive legal measure that mediates between freedom of speech and defamation in the context of online communication.

II. ANALYZING ISSUE IN CAMBODIA'S LEGAL LANDSCAPE: DEFAMATION AND FREEDOM OF SPEECH

To have a clear understanding of the legal issues, we shall look at all of the existing laws that govern freedom of speech and defamation. According to Article 41 of the constitution law, Khmer citizens shall have freedom of expression, where no one shall exercise this right to infringe upon the rights of others. Nonetheless, Cambodia has also ratified some international treaties, including the International Covenant on Civil and Political Rights (ICCPR), where Article 19 states that everyone shall have the right to freedom of expression, including seeking, receiving, and imparting information through any means.

In Criminal Code article 305, defamation is defined as any allegation or charge made in bad faith that tends to injure the honor or reputation of a person or an institution. Although Cambodia has established this definition, the law's application has yet to keep pace with technological advancements. The 2007 code, while not inherently outdated, lacks specificity in addressing defamation practices that have emerged with the rise of digital technologies.

For instance, defamation today often occurs through online platforms, where defamatory statements can reach a vast audience instantaneously. Unlike traditional forms of defamation that were confined to verbal communication or print publications, online defamation can spread rapidly and be accessed by countless individuals worldwide.[2] This shift not only magnifies the potential harm but also complicates jurisdictional issues, as defamatory content can be posted by individuals located in different countries.[3] For instance, if a user based overseas defamed an individual in Cambodia on social media. The victim will face challenges in seeking legal recourse due to the complexities of private international law. This example highlights the

[1] Kemp, Simon. "Digital 2023: Cambodia — DataReportal – Global Digital Insights." DataReportal – Global Digital Insights, February 13, 2023. https://datareportal.com/reports/digital-2023-cambodia#:~:text=There%20were%2011.37%20million%20internet%20users%20in%20Cambodia%20in%20January,percent)%20between%202022%20and%20202.

[2] Abosede Olubunmi Banjo and Dokunmu Oluwaseun Olasunmbo, "Implications of Application of the Law of Defamation in Social Media Information Dissemination," *International Journal of Social Science Research and Anthropology* 12, no. 6 (February 2023): 181-188, accessed May 30, 2024, https://www.researchgate.net/publication/370363969_IMPLICATIONS_OF_APPLICATION_OF_THE_LAW_OF_DEFAMATION_IN_SOCIAL_MEDIA_INFORMATION_DISSEMINATION.

[3] Ibid.

need for more specific legal provisions that address the global reach and immediate impact of online defamation, ensuring that victims have a clear path to justice regardless of geographical boundaries.

In bolstering Cambodia's ongoing economy, the Cambodian government finally enacted the law on consumer protection on November 2, 2019, to ensure the protection of consumers and the protection of fair competition.[4] Although the legislation has been duly enacted, it is significant to highlight the lack of provisions addressing circumstances where consumers may wish to voice suggestions or complaints about a business owner online. Thus, Cambodian law shall be modified to answer the new issue by taking a look at the developed countries that have made new interpretations concerning defamation in digital eras.

III. PROPOSED LEGAL FRAMEWORK

1. SINGAPORE'S DEFAMATION ACT

Let's take a look at one of the developed countries in Southeast Asia. Singapore has been trying to balance freedom of expression and protection against defamation in digital eras through a combination of legal frameworks. The legislative rules provide the primary legal basis for handling defamation cases and are supplemented by statutory provisions found in the Defamation Act.[5] This act highlights the legal framework for bringing defamation claims and provides remedies for individuals or businesses who have been defamed. Although Singapore recognizes freedom of speech as a fundamental right, it can be restricted in certain circumstances, especially in a case to prevent defamation.[6] The government has also adopted a nuanced approach to balancing this right with the need to protect individuals and businesses from harmful speech.[7] With this being said, they had set up a clear line that freedom of speech cannot be used as an excuse to defame someone, and individuals can receive protection from being defamed as well.

In addition to legislative measures, Singapore has a robust legal system that allows individuals and businesses to seek redress for defamation through civil litigation. Instead of having the act criminalized like in Cambodia, Singapore had characterized it into two, civil and criminal action.[8] For example, any act that is conducted without intention and deemed to be defamation can go through civil action, which makes it less severe since people might not be aware that what they stated online is deemed to defame another person's reputation.[9]

In addition, the courts are essential in deciding defamation cases because they apply legal standards to evaluate whether a statement qualifies as defamatory and, if necessary, calculate damages or other remedies.[10] Also, since Singapore is a former British colony, Singapore law follows the British common law, and defamation criteria are defined like those of Britain and the United States. For example: Defamation happens only if:

- The words were defamatory in that they injured the person's reputation either directly or by innuendo
- The person harmed by the words is proven
- The words are "published", which means that others read or heard the speech[11]

[4] Cambodia Law on Consumer Protection, Article 1.
[5] "Defamation Act 1957 - Singapore Statutes Online," April 1, 2022. https://sso.agc.gov.sg/Act/DA1957.
[6] SingaporeLegalAdvice.com. "Right to Freedom of Speech and Expression in Singapore: Myth or Reality? - SingaporeLegalAdvice.Com," January 23, 2024. https://singaporelegaladvice.com/law-articles/right-to-freedom-of-speech-and-expression-singapore#:~:text=Does%20the%20Right%20to%20Freedom,citizens%20are%20granted%20this%20right.
[7] Ibid.
[8] Ben. "Defamation in Singapore - PKWA Law." PKWA Law LLC, August 10, 2022. https://pkwalaw.com/defamation-in-singapore/#:~:text=Under%20the%20Defamation%20Act%2C%20a,the%20circumstances%20of%20the%20case.
[9] Ibid.
[10] Ibid.
[11] Melnychenko, Oleksandr. "Defamation Law of Singapore — StartupDecisions." StartupDecisions, January 26, 2024. https://www.startupdecisions.com.sg/singapore/business-laws/defamation-law.

Within the last requirement mentioned above, content communication must be at least made to one-third party, not just its mere existence and publication, which must vary with different platforms, especially concerning internet defamation.[12]

In the case of Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd, the court accepted Facebook posts as published content without detailed analysis. This case suggests that posts on social media platforms like Facebook and Instagram are considered published upon posting.[13] However, the court ruled differently in Qingdao Bohai Construction Group Co Ltd v Goh Teck Beng. They stated that the mere uploading of material online isn't enough; it must also be accessed and read by a third party in the jurisdiction where the plaintiff is suing.[14] This position aligns with several Singaporean and English decisions, and to reconcile these differences, the position in Kairos could be limited to social media, where interactions like "likes" or comments indicate access. Such indications are necessary for the general proposition in Qingdao to prevail.

This classification was very specific and tight compared to the definition in the Cambodian Criminal Code. In Singapore, there is a lot to be proven, and wrongly accused defendants may find a way to prove themselves as well.

2. EUROPEAN UNION DIRECTIVE ON CONSUMER RIGHTS

To combat defamation and safeguard customers' right to free speech, the European Union (EU) has passed several regulations and directives, especially regarding consumer protection. The Directive on Consumer Rights is an integral part of the law that protects customers' freedom to openly express their ideas without fear of being sued for defamation by companies.[15]

As mentioned in the introduction to the issues above, some people may want to use their right to free speech to shield their wrongdoing. For instance, online reviews significantly influence consumer purchases, leading some business owners to post fake reviews to boost their own products' reputations or harm their competitors. As the importance of reviews grows, so does the temptation to manipulate them.[16] Within this issue, the EU has clarified that the primary responsibility for fake reviews lies with the business owner who promotes and benefits from them, whether these reviews are positive or negative. However, identifying the trader responsible for promoting fake reviews, especially negative ones, is often difficult.[17] When fake reviews are posted by an upset customer or a private individual with no business interests, consumer protection and advertising regulations do not apply. Instead, these reviewers may be held responsible for violating the seller's right to honor under civil or criminal laws.[18]

In practice, individual consumers often lack the incentive to litigate against powerful tech companies due to the time, financial resources, and low chances of a favorable outcome. However, the New Deal for Consumers aims to empower consumer and user associations to seek redress such as compensation, replacement, or repair on behalf of groups harmed by illegal commercial practices.[19]

Additionally, the European Union's Charter of Fundamental Rights has clauses safeguarding information and speech freedom, enhancing the freedom of consumers to voice their thoughts without unwarranted

[12] Li, Fong Wei. "How the Internet Is Reshaping Defamation Laws - The Singapore Law Gazette." The Singapore Law Gazette, June 16, 2020. https://lawgazette.com.sg/feature/internet-reshaping-defamation-laws/.
[13] Golden Season Pte Ltd and others v Kairos Singapore Holdings Pte Ltd and another, [2015] SGHC 38
[14] Qingdao Bohai Construction Group Co Ltd v Goh Teck Beng, [2016] SGHC 142.
[15] "Consumer Rights Directive." European Commission. https://doi.org/https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/consumer-rights-directive_en.
[16] Martínez Otero, Juan María. "Fake Reviews on Online Platforms: Perspectives from the US, UK and EU Legislations." SN Social Sciences 1, no. 181 (2021): 1-30. https://doi.org/10.1007/s43545-021-00193-8.
[17] Ibid.
[18] According to the UCPD, the Directive does not apply to consumers who provide information or misinformation about their experience with products or services unless they are acting on behalf of a trader. This is because the UCPD applies to any natural or legal person that qualifies as a "trader," according to Article 2(b) UCPD.
[19] European Commission. Proposal for a Directive of the European Parliament and of the Council on Representative Actions for the Protection of the Collective Interests of Consumers, and Repealing Directive 2009/22/EC. COM/2018/0184 final.

interference.[20] The EU's Charter of Fundamental Rights, regularly scrutinized by legal scholars and human rights experts globally, is esteemed for its robust protection of freedom of speech and information. Its principles, deeply entrenched in democratic values, serve as a touchstone for international human rights standards. Although these statutes do not specifically cover defamation lawsuits between companies and customers or companies and companies, they create a thorough legal framework that protects consumers' right to free speech while providing sufficient protection from defamation.

On another note, for the United Kingdom, under the Defamation Act 2013, severe negative fake reviews may lead to libel suits. For legal action to be pursued, the fake review must cause "serious harm," resulting in a significant financial loss according to Article 1 of the Act.[21]

3. DIFFERENT APPROACHES TO DEFAMATION LAWS AND FREE SPEECH PROTECTION IN GLOBAL JURISDICTIONS

There is a causal link between a defamatory post and subsequent economic loss, as businesses often fall off steeply after having received any defamatory claim.[22] The Australian Competition and Consumer Commission responded to this issue by outlining in great detail how a company must handle the review to comply with consumer law. They suggested that companies take complaints about false or deceptive evaluations seriously on their websites or social media accounts. They have the option to ask the platform to remove or reply to a fraudulent review if they come across one. Both businesses and platforms could get in trouble if they don't remove fake reviews they know about after making sure first that a review is indeed fake.[23]

On the other hand, the Indian Penal Code (IPC) and the Information Technology Act (ITA) are the main rules that deal with defamation. India has interpreted and applied defamation laws to address online defamation cases, recognizing the unique nature of digital communication and its potential to reach a wide audience instantly. Moreover, it also addresses the issues with the intermediary liability, which complies with the EU directive consumer. When people make untrue statements on social media, blogs, or websites, it's considered defamation in the digital world. Usually, if a harmful statement is shared online, it's regarded as online defamation. For instance, if someone posts or spreads false things about a person or a company on platforms like Facebook, WhatsApp, or Instagram, it's called cyber defamation.[24]

Moreover, in the US, if the comment or review harms the integrity of the shop owner, it can be brought under the Defamation law based on the regulation in each state. However, the actual harm has to be proven, and a written defamatory factual statement has to be presented.[25] It simply meant that mere online publications or implied posts cannot be deemed defamation.

IV. RECOMMENDATION FOR AMENDING CAMBODIA'S LEGAL FRAMEWORK

To address the legal challenges posed by defamation and freedom of expression in the digital age, Cambodia can draw valuable insights from the practices of other jurisdictions. Singapore's Defamation Act balances the right to freedom of speech with protection against defamation and offers a clear legal framework for handling such cases. By adopting a similar approach, Cambodia can establish specific guidelines for online defamation, ensuring that both individuals and businesses are protected without infringing on free speech. In addition to that, Cambodia could also promulgate a new criminal code to

[20] European Union Charter of Fundamental Rights, Article 11.
[21] UK. Defamation Act 2013. Chapter 26. https://www.legislation.gov.uk/ukpga/2013/26/contents
[22] Davis Business Law. "Handling Business Defamation: A Guide to Protecting Your Company's Reputation," January 9, 2024. https://davisbusinesslaw.com/handling-business-defamation-a-guide-to-protecting-your-companys-reputation/#:~:text=Legal%20Remedies%20for%20Defamatory%20Statements&text=This%20may%20include%20reimbursement%20for,to%20its%20pre%2Ddefamation%20state.
[23] Australian Competition and Consumer Commission. "Online Product and Service Reviews," March 28, 2023. https://www.accc.gov.au/business/advertising-and-promotions/online-product-and-service-reviews.
[24] Partners, Legal Eye. "Defamation Laws in the Digital Age: Balancing Free Speech and Online Reputation.," January 18, 2024. https://www.linkedin.com/pulse/defamation-laws-digital-age-balancing-free-speech-online-wzucc?trk=article-ssr-frontend-pulse_more-articles_related-content-card.
[25] California Civil Code §§ 45 to 47.

make the provision for defamation as strict as Singapore's. By doing so, there will be many criteria for both the defendant and the plaintiff to find proof.

Additionally, the European Union's Directive on Consumer Rights emphasizes the need to safeguard consumers' freedom to express their opinions while preventing the spread of false information. Cambodia could implement a comparable directive that specifically addresses the spread of misinformation on digital platforms, providing mechanisms for swift redress and clear penalties for violations.

Moreover, Australia's detailed approach to managing online reviews can serve as a model for Cambodia's effective handling of consumer complaints. Implementing a system that requires platforms to take down false reviews promptly and provides legal recourse for affected parties would strengthen consumer protection.

V. CONCLUSION

In conclusion, the intersection of freedom of expression and protection against defamation in the consumer protection context has a complex legal landscape that requires an adaptive measure. While Cambodia has existing legal frameworks such as the Criminal Code and Consumer Protection laws, there remains a gap in addressing online defamation specifically. To bridge the pointed gap, it is significant to propose clear legal measures aligning with the nature of online communication. Drawing from examples such as Singapore, the European Union, Australia, and India, we can gain insight into how different jurisdictions approach the balance between freedom of expression and protection against defamation in the context of consumer protection.

However, challenges and implications still occur, including difficulty navigating the legal process and the need for more resources to amend the law. It is indisputable that Cambodia is a developing country shifting into the digital era with limited human resources. Considering and modifying the law to address these current issues will take time.

Overall, addressing the dynamic landscape of freedom of expression and defamation in the consumer protection context requires a multifaceted approach that balances fundamental rights with the need to protect individuals and businesses from harm.

Source: Thompsonsoncoburn

ADDRESSING ONLINE MISINFORMATION IN CAMBODIA: BALANCING REGULATION AND FREEDOM OF SPEECH

CHHENG Khema
is a 2023 graduate of the English Language Based Bachelor of Law Program. She is also currently pursuing her senior year in International Relations at the Institute of International Studies and Public Policy. She has been working as a lawyer assistant in the litigation field for two years. Besides her education and experience in the law field, she is also interested in diplomacy and once joined Mekong's Youth Diplomacy Simulation.

I. INTRODUCTION

Cambodia has integrated digital technology into daily communication, work, and access to information. Out of approximately 17 million people, there were 11.37 million internet users and 10.95 million social media users.[1] There were registered media outlets, including 661 newspapers and magazines, 878 online news websites and programs, 221 FM radio stations, 19 TV stations, and 165 relays TV stations.[2] A report on "Information Disorder" by Wardell and Derakhshan from the Council of Europe defined misinformation as false information made without the intention to harm. It escalates when an individual or journalist spreads false information about a rumor or an event without knowing its falsity.[3] The issue is not how digital evolution impacts the flow of information; it is how that piece of information is defined as misinformation. Online misinformation is an emerging issue; consequently, many societies are challenged by legal ambiguity as a result of unclear definitions and descriptions.[4] Instead, there is a report of seventy-eight countries introducing anti-false news with common approaches like imposing fines and imprisonment on the offender, taking down the contents, and some of them focus on enhancing media transparency and literacy.[5]

In Cambodia, there is no comprehensive law on the distribution of information; however, the Ministry of Information has initiated an effort to detect more than 6000 online polluted news[6] and regulate the advertisements. The lack of law to manage information flow causes uncertainty in standardizing information and determining if it is misinformation. This research paper aims to study how Cambodia has handled misinformation, with the understanding that the audience, as legal professionals, policymakers, and researchers, plays a crucial role in shaping the future of this issue.

- What are the legal implications of the anti-fake news approach to freedom of speech?
- What is the way to mitigate online misinformation without infringing freedom of speech?

II. FRAMING THE ONLINE MISINFORMATION IN CAMBODIA

"Misinformation" is not as familiar as "false news" in Cambodia. There is no definitive interpretation of misinformation, but it is commonly seen as false information with misleading content disseminated to earn attention or confuse the audience because they think it is true.[7] The term "misinformation" originally describes the nature of the information, including whether it is erroneous, lacking, or incorrect.[8] The definition varies; an ASEAN Digital Literacy Program report claims that Cambodian youths have understood misinformation as false information aimed to deceive and take advantage of others. [9]

Cambodia has no explicit law on misinformation; therefore, the absolute definition of the term in the legal context has yet to exist. Countries like South Korea regard false news as both civil and criminal wrongdoing;[10] however, Cambodia's legal framework criminalizes the dissemination of false news. Instead of referring to the act as misinformation, our most-used term is "false information" based on Article 425

[1] The Fifth Cambodia ICT and Digital Forum. CamIDf, January 02, 2024. https://camidf.net/article/the-fifth-cambodia-ict-and-digital-forum
[2] Increasing number of media outlets reflects freedom of expression and press freedom in Cambodia. KHMERTIMES, April 06, 2023. https://www.khmertimeskh.com/501269087/increasing-number-of-media-outlets-reflects-freedom-of-expression-and-press-freedom-in-cambodia/
[3] Claire Wardle and Hossein Derakhshan. 2017. "Information Disorder: Toward an interdisciplinary framework for research and policymaking." Council of Europe report, DGI (2017) 9 (2017).
[4] Chan, Eugene. 2023. "Analysis of the Challenge in Fake News and Misinformation Regulation Comparative in Global Media Landscape" 178 (January): 02018–18. https://doi.org/10.1051/shsconf/202317802018.
[5] Lim, Gabrielle, and Samantha Bradshaw. 2023. "Chilling Legislation: Tracking the Impact of 'Fake News' Laws on Press Freedom Internationally." Center for International Media Assistance. July 19, 2023. https://www.cima.ned.org/publication/chilling-legislation/.
[6] Ministry's stats point to a steady rise in fake news. The Phnom Penh Post, April 09, 2023. https://www.phnompenhpost.com/national/ministrys-stats-point-steady-rise-fake-news
[7] Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information. Journalism, 'Fake News' & Disinformation". UNESCO, 2018, p44 https://en.unesco.org/sites/default/files/f._jfnd_handbook_module_2.pdf
[8] Fallis, Don. 2015. "What Is Disinformation?" Library Trends 63 (3): 401–26. https://doi.org/10.1353/lib.2015.0014.
[9] One Divide or Many Divides? Underprivileged ASEAN Communities' Meaningful Digital Literacy and Response to Disinformation. n.d. ASEAN Foundation. Accessed May 31, 2024. https://www.aseanfoundation.org/one_divide_or_many_divides_underprivileged_asean_communities_meaningful_digital_literacy_and_response_to_disinformation.
[10] Chan, Eugene. 2023. "Analysis of the Challenge in Fake News and Misinformation Regulation Comparative in Global Media Landscape" 178 (January): 02018–18. https://doi.org/10.1051/shsconf/202317802018.

of the Penal Code. From the report of Wardell and Derakhshan, misinformation is unintentional to harm others but contains misleading content. Meanwhile, "false information" in the Criminal Code narrowly explains it as the disclosure of misleading information that destroys, defaces, and damages others.[11] No further legislation provides on what elements constitute misinformation; the interpretation varies as the law is open to both individuals and national entities filing cases of misinformation. Notably, the individual and national institution can bring the case to the court when they find any disseminated false information deemed to degrade their dignity; the verdict on whether the accused is guilty depends on the judge's discretion to decide.

1. APPLICABLE LEGISLATIONS FOR REGULATING ONLINE MISINFORMATION

Due to the absence of a law that specifically deals with misinformation, there are pre-existing legislations below to restrict information disorder and strengthen the ethics of journalism.

- Constitution

Freedom of expression and press is protected under Article 41, yet it is limited to exercising the right to violate other individuals and society's order. Additionally, the expression in the media outlet shall be determined by a specific law.[12] This article aligns with Article 19 of the International Covenant on Civil Political Rights (ICCPR) as it both guarantees the freedom of speech and restricts certain actions. Article 19 (3) of the convention limits what infringes on the rights or dignity of others and public orders.[13] Therefore, these top-tier legislations bind the government to respect freedom of speech and impose restrictions provided by law if necessary.

- Criminal code

The public exhibition of false information deemed harmful to an individual's dignity is subjected to imprisonment from one to two years and a fine from two million to four million Riels[14]. Additional penalties may be imposed according to Article 426.[15] The provision is not precise as the main components of the Penal Code are provisions on crime and penalty. It does not identify what makes it false information; instead, it focuses on only criminalizing the act. Does the information have to be entirely or partially false? It is only a crime when the action is provided in law, materialized, and intended. What if the original poster does not intend to harm anyone but legitimately spread awareness? It is still subject to the discretion to decide whether it is misinformation.

- Law on Press

Some nations have utilized existing provisions on defamation to protect people and the public from the detrimental purposes of false news. For instance, the South Korean constitution safeguards people from being defamed or having their reputations damaged while exercising their right to free expression.[16] Meanwhile, Cambodia refers to defamation through the media as being the competence of the Law on Press. If the published content obtains false information that humiliates an individual or public figure, the victim can demand the publisher to issue a retraction within seven days, or else they can seek compensation via court.[17] The law also punishes press publication of false information that shames public institutions with a fine of two million to ten million riels.[18] On the bright side, the law stipulates the responsibility of journalists in Chapter II to promote professionalism and ethics in journalism. Plus, it does not impose imprisonment or additional penalties like the Penal Code.

[11]Criminal Code of Cambodia, Article 425
[12]Constitution of Kingdom of Cambodia, Article 41
[13]International Covenant on Civil and Political Rights (ICCPR), Article 19(3)
[14]Criminal Code of Cambodia, Article 425
[15]Ibid.
[16]Chan, Eugene. 2023. "Analysis of the Challenge in Fake News and Misinformation Regulation Comparative in Global Media Landscape" 178 (January): 02018–18. https://doi.org/10.1051/shsconf/202317802018.
[17]Law on Press of Cambodia, Article 10
[18] Law on Press of Cambodia, Article 13

2. THE LOOPHOLE OF THE PRACTICE

Strict scrutiny demands that speech-limiting legislation be written narrowly to prevent speakers from speaking the truth or from giving government authorities a chance to punish them differently based on their opinions.[19] These approaches to criminalization frequently fail to make a distinction between speech that is permissible and speech that is unlawful, restricting the practice of free speech and giving governments more power and discretion.[20] A law cannot grant those in charge of carrying out unrestricted choice over how to limit the freedom of expression. Laws must offer those tasked with enforcing them enough direction to determine what forms of speech are appropriately limited and what kinds are not.[21] Due to the law's ambiguous wording, the interpretation is subjective, which may undermine the right to free speech and make some forms of communication illegal.[22] Specifically, the terms in the Criminal Code as the proper definition are limited. Criminal Law instead handles cases of misinformation under defamation or incitement. The Penal Code imposes punishment heavier than Law on Press as it includes both principles of penalty (fine and imprisonment), and additional penalties are available.

III. CHALLENGES AND WAY FORWARD

H.E. Neth Pheaktra, the minister of the Ministry of Information, addressed the lack of a legal framework to put up with the information flow in the emergence of digital development in the Closing Ceremony of the Ministry of Information's 2023 Work Review Meeting and 2024 Work Implementation Directions. In response to this issue, one of the ministry's missions is to establish updated legal frameworks for the social context. These are the Draft Law on Access to Information (A2I) and the current Law on Press amendment. He also included empowering journalism with the future legal framework called the "Charter of Professional Journalism" to improve ethical conduct, advertisement, online issuance, and broadcast outlets.[23] In the Conference on Freedom of Press in April, the Ministry of Information announced to ensure a safe atmosphere for media and professional journalists in Cambodia to advocate press freedom on the principles of equality, non-discrimination, non-intimidation, and non-political affiliation.[24]

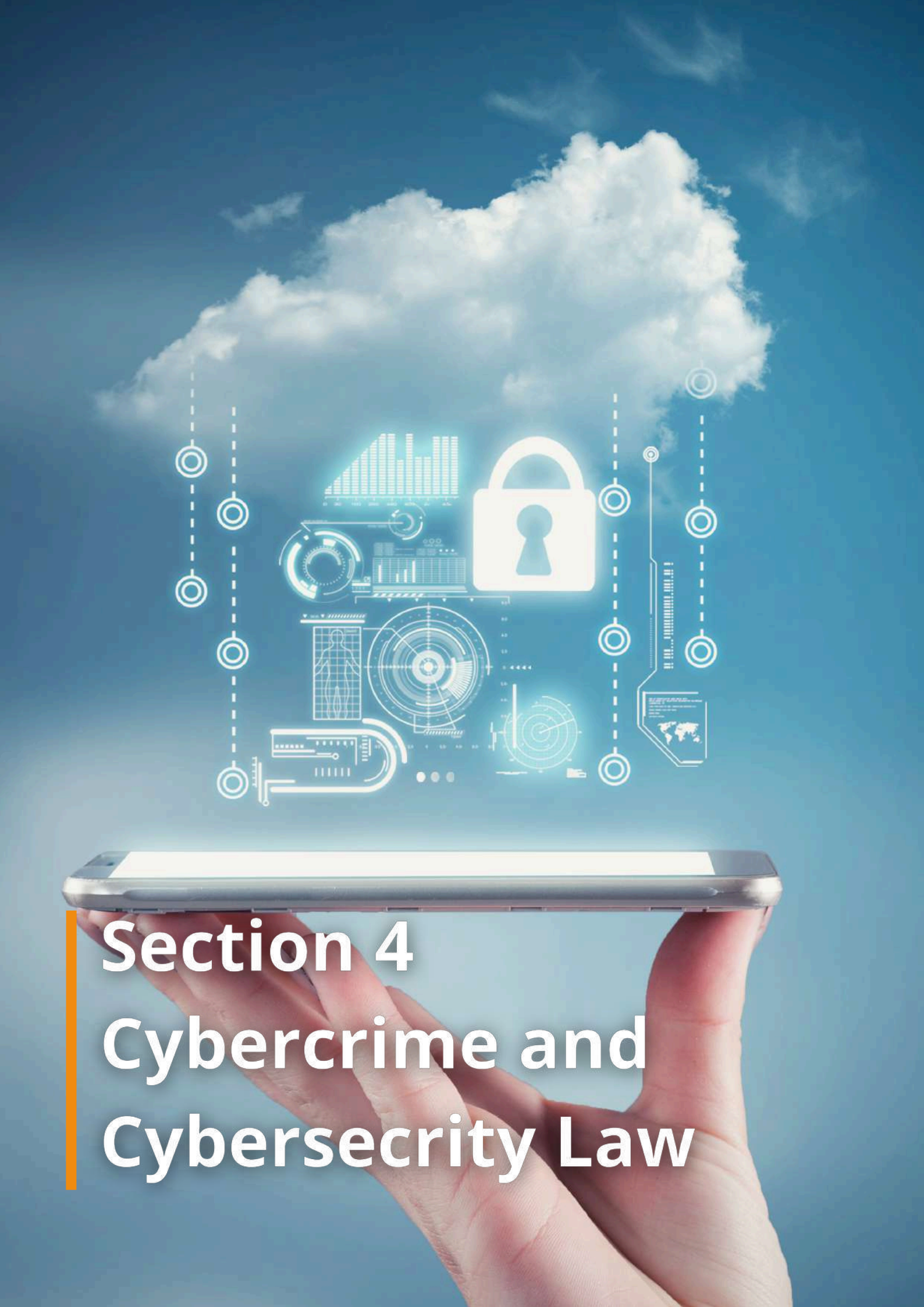
Pushing Cambodians to be digital citizens is one of the missions in Cambodia's Digital Economy and Society Policy Framework 2021-2035. However, our digital literacy is still limited. The capacity to utilize digital devices for communication, information exchange, and Internet search is only approximately 30% of Cambodians. To ensure reliable information, the interaction between line ministries and citizens has increased through sharing information and documents via Telegram and WhatsApp to overcome the spread of false information, incitement, and outdated information.[25]

IV. CONCLUSION

With the benefit of digital transformation, the distribution of false information in platforms is imposing a challenge to society with limited digital literacy and incongruous legal frameworks. The problematic parts of dealing with online misinformation are the vague definition, absence of specific law, and subjective interpretation.

The Ministry of Information recognized the need to update or amend the current Law on the Press to respond to the digital transformation effectively. It is also a must to ensure that upcoming laws or regulations aimed at preventing misinformation are appropriately drafted to avoid conflicting with the freedom of speech. The respective ministry also proposed the Charter of Professional Journalism to enhance ethical journalism and advocate inclusivity. Moreover, the interaction between the government's entities and public citizens also increases digital literacy by exchanging and confirming the news.

[19] United States v. Alvarez, 567 U.S. 709, 731–32 (2012) (Breyer, J., concurring) (quoting 567 U.S. at 751 (Alito, J., dissenting).
[20] Vermeulen, Mathias. n.d. "IS THAT the QUESTION? ONLINE CONTENT: TO REGULATE or NOT to REGULATE." https://www.apc.org/sites/default/files/OnlineContentToRegulateOrNotToRegulate.pdf.
[21] Human Rights Committee, General Comment No.34, note4, para 25
[22] International Center For Not-For-Profit Law. Legal Analysis: Draft Law on Cybercrime 2022 (Cambodia). September 2022.
[23] H.E. Neth Pheaktra in the Ministry of Information's 2023 Work Review Meeting and 2024 Work Implementation Directions, on 23 January 2024.
[24] H.E. Neth Pheaktra in Conference on Freedom of Press, on 30 April 2024
[25] Cambodia's Digital Economy and Society Policy Framework 2021-2035, May 2021



Section 4
Cybercrime and Cybersecrity Law

Source: JJayant Singh RRajput

PROTECTING DIGITAL DOMAIN BY LAW ON CYBERCRIME: LEGAL REMEDY AGAINST CYBER HARASSMENT IN CAMBODIA

VUN Samadarin

is a program manager of English Language Based Bachelor and Master of Law (ELBBL-ELBML) at the Royal University of Law and Economics (RULE); where she holds two bachelor's degrees, law in Khmer language program and law in ELBBL program. She is also a research assistant for a project "Justice Transition after the Khmer Rouge Region" for two PhD candidates in Canada and Germany. She was an Honorable Delegate and was appointed as Asia Youth Innovator Ambassador and Honorable Academic Innovation Presenter at the Japan International Youth Innovation Summit 2024 in Tokyo. With a passion for human rights, she worked as a research intern at the Center for the Study of Humanitarian Law (CSHL) where she published newsletters and now processing the publication of a research paper on business and human rights.

I. INTRODUCTION

The increasing use of digital and new technology disturbs individuals' daily lives with cyber risks such as cybercrime and data protection issues[1] and leads to online harm, including cyber harassment.[2] As more aspects of daily life rely on the Internet, aggressive acts like harassment also increase through electronic media.[3] Cyber harassment in Cambodia is not explicitly outlined in specific regulations. Still, it covers the base definition under the Criminal Code of Cambodia, including "public defamation" and "insult" in articles 305 and 307, respectively. Law on Telecommunication also criminalizes a repeated act of "threatening" to commit a crime[4] or to destroy the property of others.[5]

Harassment through the internet has been growing in the past few years due to convenience and comfort in internet usage, which has seen widespread developments of cybercrimes along with it.[6] Among Cambodian females aged 15 to 65 of age, 29 percent have experienced online harassment: being called offensive names, criticized, embarrassed, physically threatened, sexually harassed, and unwanted contact.[7] Moreover, a study from the United Nations Children's Fund (UNICEF) found that 85.7 percent of Cambodian youth from age 15 to 25 are at risk of online harassment, with LGBT+ groups having a high rate of being the victim.[8]

Nevertheless, some have observed that Cambodia has not implemented a Law on Cybercrime to deal with cyber-related issues yet because of controversy regarding human rights in the early stage.[9] In the meantime, any crime committed through the internet or telecommunication, the proceeding of legal remedies and penalties, falls first under the Code of Criminal Procedure and Criminal Code of Cambodia.

In contrast, even Cambodian laws mention and criminalize acts that could be considered cyber harassment, but it still lacks a significant specific legal framework that directly addresses cybercrimes. It also leaves individuals vulnerable to online abuse, and without clear laws, it may be challenging for victims to seek protection and justice. So, a dedicated Cybercrime Law would benefit the government in combating modern threats as Cambodia, like other countries, faces growing cybercrimes due to reliance on digital technologies and the Internet. Moreover, it would aid the protection of national security from unaccountable risks in government systems like targeting critical infrastructure and sensitive information by equipping authorities with the tools needed to safeguard national security interests with the specific Cybercrime Law.

Therefore, this paper will address related Cambodian and International laws on cyber harassment to analyze the remedies that victims may rely on. Furthermore, how effective are those existing remedies, and what does Cambodia need to advance to combat cybercrimes effectively?

II. FEDERAL LAWS AND STATE LAWS IN THE UNITED STATES ON CYBER HARASSMENT

U.S. Federal laws refer to the body of legal rules and regulations established to apply throughout the United States. It also includes court decisions and regulations issued by federal administrative agencies.[10] Federal laws also address various forms of cybercrimes, such as online abuse. These laws include provisions against using the internet to harass or stalk someone severely, making threats across state

[1] Open Development Cambodia, "Science and Technology policy and administration", June 7, 2022,
Science and technology policy and administration | Open Development Cambodia (ODC).
[2] Stevens Francesca, Nurse Jason R.C., Arief Budi, "Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review", Cyberpsychology, Behavior, and Social Networking, 2020.
[3] Slaughter A., & Newman E., "New Frontiers: Moving Beyond Cyberbullying to Define Online Harassment", Journal of Online Trust and Safety, Vol. 1 (2), 2022, pp. 1-25.
[4] Law on Telecommunication, Art. 93.
[5] Ibid, Art, 95.
[6] Sati Mehul, "Cyber Crimes and Harassment of Women: An Analysis of the Legal Framework", August 21, 2023, pp.3-4.
[7] Monyvann Nhean, "The current situation of online GBV harassment in Cambodia", Ideas for Peace,
The current situation of online GBV harassment in Cambodia – Ideas for Peace.
[8] Ibid.
[9] Open Development Cambodia, "Science and Technology policy and administration", op.cit.
[10] United States Law, "US Law", Justia.
United States Law :: US Law :: Justia

lines, hacking, identity theft, and using electronic communication services to engage in a course of conduct causing substantial emotional distress.[11] The U.S. legal framework covers a wide range of forms of online harassment in several federal laws, addressing all online abuses by dividing the forms into definitions and penalties.

The Cambodian government has adopted international frameworks and enacted domestic laws to prevent violence in various crimes. However, online harassment remains a gray area lacking clear definitions because the Cambodian Law on Cybercrime is still in draft.

As the U.S. is often considered the next level in cybersecurity and combating cybercrimes, Cambodia adopting the Law on Cybercrimes by looking up international practices like US federal laws may help address cyber threats and develop well-made cybercrime legislation in Cambodia. Moreover, understanding the various forms of online harassment and the applicable laws at both the national and international levels is significant for addressing this issue effectively in Cambodia.

1. FEDERAL LAWS

Although there are no specific federal cyber harassment laws, the U.S. government has a law on cyberstalking in 18 U.S. Code section 2261A.[12] The law imposes penalties for someone using a computer or electronic communication system to intentionally injure, intimidate, kill, harass, or surveil another person. The section prohibits perpetrators from using the internet to harass or stalk someone with severe action; otherwise, they hold responsibility with a fine and imprisonment for not more than five years.[13] It also imposes on using the internet to place someone in fear of "death or serious bodily injury" or causes or attempts to cause mental distress.[14] Additionally, 18 U.S. Code Section 875 imposes the same penalty when someone transmits interstate or communication with any threat to kidnap or injure another person, meaning making threats across states.[15] This law applies to all crimes committed in different states between perpetrator and victim with the same penalty as Section 2261A of the 18 U.S. Code.

Concerning harassing, threatening phone calls and sending harassing or threatening messages across states, there is a law of 47 U.S. Code Section 223 to imply.[16] This law is to prohibit any act of using a telecommunications device to abuse, threaten, or harass a person intentionally. Besides, there is a law that prohibits hacking, such as the Computer Fraud and Abuse Act in 18 U.S. Code Section 1030.[17] In the case of accessing a computer without authorization or consent to get information and intent to cause damage, it shall fall under penalties of imprisonment up to one year or up to five years in case of gaining private finances.[18] For instance, when a person intentionally uses a computer that belongs to another person without the other party's consent or permission, this law will apply with the stated penalty. The case of gaining private finances refers to fraud through a computer to obtain some finance for personal usage, which will result in imprisonment of up to five years.

Additionally, in the matter of using another person's identification documents intentionally without lawful authority, Section 1028 of the 18 U.S. Code was established to prohibit such action.[19] The crime comes with penalties of a fine and imprisonment for not more than fifteen years, not more than twenty years if committed in connection with violence or after a prior conviction under this section.[20] Although there is no mention that this law applies specifically to cybercrime, it covers all the information in case of such a crime committed, including through telecommunication or the internet.

[11] Title 18 and 47 of the United States Code and New York Penal Law.
[12] Title 18 of the United States Code, Section 2261A.
[13] Title 18 of the United States Code, Section 2261A.
[14] Wisselman Harounian, "Laws on Cyberbullying & Cyberstalking", Wisselman Harounian Family Law, Laws on Cyberbullying & Cyberstalking - Wisselman, Harounian & Associates (lawjaw.com).
[15] Title 18 of the United States Code, Section 875.
[16] Title 47 of the United States Code, Section 223.
[17] Title 18 of the United States Code, Section 1030.
[18] Ibid.
[19] Title 18 of the United States Code, Section 1028.
[20] Ibid.

2. STATE LAW OF NEW YORK PENAL LAW

While no federal laws directly target online harassment, US states have legislation enacted to address related behaviors. For instance, cyber harassment is considered a Class A misdemeanor resulting in up to one-year imprisonment and fines under the Crime of Aggravated Harassment in the second degree of NY Penal Law Section 240.30, New York.[21] It considers cyber harassment to occur when a person communicates by transmitting or delivering any form of written communication via electronic with the intent to "harass, annoy, threaten, or alarm another person" or to a family or household member physically.[22]

The several federal laws specifying online harassment and abuse in the existing laws address and cover different forms of online harassment. One of the laws also states that causing substantial emotional distress is a crime with a fine and imprisonment. It showcases the Federal Laws detailing the crime with definitions, which aims to protect individuals from being vulnerable to cyber harassment.

III. CAMBODIA LEGAL REMEDY ON CYBER HARASSMENT

Cyber harassment is a crime that would typically fall under the Law of Cybercrime. However, while the law is still in the draft phase in Cambodia, this paper will address legal actions proceeding with the existing country's laws related to crime. Overall, individuals in Cambodia have legal protections[23] and victims of cyber harassment may file a court complaint through various laws, including Criminal Procedure and Civil Procedure for civil action in damages and the Criminal Code and Law on Telecommunication for Criminal Liability.

In order to have a discussion, it is essential to analyze and understand the scope of existing laws regarding cyber harassment and how effective the remedy is for victims within the legal framework.

1. CRIMINAL LIABILITY

Cyber harassment has not yet been defined under Cambodian law. However, according to international definitions, the term crime can be found in various articles of the Criminal Code and Law on Telecommunication.

Public defamation is stated in Article 305 of the Criminal Code of Cambodia that any allegation or slanderous charge that undermines the honor or reputation of a person or an institution constitutes defamation.[24] Similarly, outrageous expression, any contempt or invective, even not affect slanderous charges, shall be considered an "Insult".[25] The defamation and insult that was committed by speeches, writing or sketches, or any means of audio-visual communications in a public place or exposed to public sight is punishable by a fine.[26]

In addition, any threatening to commit a crime or felony[27] and threatening to destroy others' property,[28] and if the threat is committed repeatedly through telecommunication, shall be sentenced in prison and fined, with or without identifying themselves.[29]

Despite all the articles that have not directly mentioned cyber harassment, those crimes are considered a type of cybercrime in the context of cyber harassment if committed through a computer network. Existing laws, though with no clear definition, shall indicate a punishment for harassment through the Internet while Cambodia is still in the process of finalizing the law targeting cybercrimes.

[21] New York Penal Law, Section 240.30.
[22] Ibid.
[23] Constitution of Cambodia.
[24] Criminal Code of Cambodia, Art. 305.
[25] Ibid, Art. 307.
[26] Ibid, Art. 305 & 307.
[27] Law on Telecommunication, Art. 93.
[28] Ibid, Art. 95.
[29] Ibid, Art. 93 & 95.

2. CIVIL ACTION FOR DAMAGE

Nonetheless, repeatedly receiving such disturbance matters may cause psychological and mental problems for victims who have been targeted,[30] and therefore, claiming civil compensation from offenders besides imprisonment is another way of remedy under Cambodian legal proceedings.

A victim can be compensated with a civil action in criminal cases, as mentioned by Article 13 of the Criminal Procedure Code of Cambodia.[31] To allow individuals affected by the crime, direct consequence, personal damage, or occurred and exists at the current time to seek any damage compensation resulting from criminal offense, victims have the right to file a civil claim.[32] However, it needs to proceed simultaneously with the criminal case without waiting for the criminal trial's conclusion for the claim to be effective, although the outcome of the criminal case does not determine the outcome of the civil claim. The compensation for injury damage can be physical, psychological (emotional distress), property, or financial losses.[33]

For instance, if a victim awaits a court decision on a criminal before filing civil compensation, fearing that it might affect the civil action, the proceeding of action cannot be made at all once the court issues the outcome of the criminal case.

The victim of a criminal offense can also claim compensation through a court order to receive proportionate for the injury suffered.[34] The scope of this compensation is to cover the physical, emotional, and financial damage due to the criminal act. The amount to be paid is based on the extent of the injury and the losses incurred by the victim.[35] Hence, the offender has further legal consequences if he or she fails to comply with the court order.

The Criminal Procedure ensures victims' rights to seek civil action remedies and receive adequate compensation for the harm caused by criminal activities. Legal proceedings not only provide justice but also restitution for victims' injuries.

IV. DISCUSSION TO LEGISLATE A SPECIFIC CYBERCRIME LEGAL FRAMEWORK

Despite all the mentioned legal remedies and proceedings, Cambodia has many aspects of government that effectively combat cybercrime, although no specific law details them yet.

Various definitions of cyber harassment in Cambodian law appear to lack understanding and detail of what is considered the act of cyber harassment, which may be problematic concerning prevention and protection. Furthermore, legislation absence comprehensive that specifically targets cyber offenders has left Cambodia endangered to various forms of line harassment, including stalking, threatening, and hacking, resulting in severe online abuses.

In the United States, federal laws state several forms of cybercrimes, including stalking, threats, harassment, hacking, and identity theft, and also apply to cybercrimes that are committed across states. According to the U.S. Department of Justice, there are different categories of cybercrimes and which federal agency to contact in case of internet-related crime.[36] It said that the crime should be reported to "appropriate law enforcement investigative" authorities, depending on the scope, at the local, state, federal, or international levels.[37]

[30] Omar A. Alismaiel, "Digital Media Used in Education: Influence on Cyberbullying Behaviors among Youth Students", Int. J. Environ. Res. Public Health, 2023, 20(2), 1370.
[31] Cambodia Code of Criminal Procedure, Art. 13.
[32] Ibid.
[33] Ibid.
[34] Ibid, Art. 14.
[35] Ibid.
[36] Criminal Division, "Reporting Computer, Internet-related, Or Intellectual Protery Crime", U.S. Department of Justice, Criminal Division | Reporting Computer, Internet-related, Or Intellectual Property Crime (justice.gov).
[37] Ibid.

Online harassment is a cybercrime that, if left unattended, may empower the perpetrator to encourage their behavior to severe forms of abuse such as online sexual exploitation of victims. A report back in 2021 showcased minor exploitation of "revenge pornography", a form of cyber abuse as non-consensual pornography involves online distribution.[38] Although it is not a solid case of regular online harassment, it demonstrates how far the crime could expand if unaddressed.

A case report on a minor 16-year-old girl named Sophal, who was secretly filmed by her partner while having sexual intercourse without her consent and used her social media account to share it publicly. Although later the man was sentenced to one year in prison with civil compensation of 5000$, he had not been detained in any proceeding stage nor paid the compensation.[39] This demonstrates legal proceedings in Cambodia lack effectiveness in court procedures.

With all the statistics and case reports, the government has not legally enforced authorities to prevent and protect victims sufficiently. Evidently, Cambodia does not provide adequate remedies for combating cybercrimes due to a lack of a specific legal framework addressing cyber threats.

V. CONCLUSION

Cyber harassment is growing in the digital age, with individuals targeted based on their political beliefs, gender, and age. The lack of clear definitions and specific laws contributes to the situation, exposing victims to online abuse. Moreover, court proceedings also practice ineffective procedures in online harassment, creating confusion about what constitutes cyber harassment and how it should be sought through legal remedy sufficiently due to a lack of Cybercrime Law.

There is a need for comprehensive legislation that defines cybercrimes, imposes punishments on offenders, and ensures protection for victims. Without a well-structured legal framework, cybercrime offenders may perpetuate the cycle of online abuse and make certain groups of individuals vulnerable to cyber harassment.

It is significant for the Cambodian government to have adequate protection and enforcement mechanisms to address cybercrime and cyber harassment, including preventive measures, responses to incidents, and accountability for perpetrators.

Therefore, Cambodia needs to establish comprehensive legislation specifically targeting all cybercrimes, including cyber harassment, to provide a legal basis for prosecuting offenders and protecting the rights of individuals in the digital space. By defining cyber harassment in the laws, including penalties, and outlining mechanisms for reporting such crimes, Cambodia would overcome a significant challenge for its citizens. Additionally, having a specific law on cybercrimes and demonstrating its commitment to addressing cyber threats through legislation would promote trust in the digital economy with foreign investment and foster innovation in the digital sector. Most importantly, it would help encourage individuals to be self-aware in approaching the internet, where they may be victimized.

[38] Europe Institute for Gender Equality (EiGE), "Cyber violence against women and girls", 2017, pp.2, cyber_violence_against_women_and_girls.pdf.
[39] Sorn Sarath & Ngay Nai, "Licadho report: Online harassment violates human rights, requires official and private-sector responses", CamboJa News, November 28, 2021,
Licadho report: Online harassment violates human rights, requires official and private-sector responses | CamboJA News.

Interior Minister Sar Kheng hands the stamp to newly appointed Justice Minister Keut Rith.
Source: Khmer Times

CAMBODIA'S APPROACH TO SMISHING: AN EXAMINATION OF CAMBODIA'S CRIMINAL CODE AND ITS COMPARISON WITH AUSTRALIA'S FRAMEWORK

HOK HourChhunhou
is a junior student in Bachelor of Law and a sophomore in English Language-Based Bachelor of Law at the Royal University of Law and Economics. Besides his academics, he interned at the Sala Traju Association and Fintech Center of the General Secretariat of Non-Bank Financial Services Authority, and he worked at the Center for Digital and Distance Education and at the Research Creativity and Innovation Fund of the Ministry of Education Youth, and Sport. He was the delegate at the Asian Undergraduate Symposium, Youth Ecosperity Dialogue, and UNESCO UNITWIN Legislative Forum. He used to be involved in social affairs and volunteer work in youth organizations such as UFYC and Scout, and he was passionate about working in legal education for the university student community. He is also one of the KASFLY Fellows 2024, and his fields of interest are digital law, criminal law, and cybercrime law.

I. INTRODUCTION

In the digital context, communication is growing rapidly. With the development of social media, email, text messaging, and the internet in general, individuals can instantly communicate with anyone anywhere in the world. The Department of Information Technology of the Ministry of Interior has revealed five major technological crimes, such as phishing attacks, vishing attacks, distributed denial of service attacks, identity theft, and ransomware attacks.[1] Moreover, the most common crimes are low-level crimes such as mobile phone fraud (calling to win prizes, SMS), threatening to post nude photos, stealing users data, and child pornography.[2] According to the Anti Cybercrime Department of the Ministry of Interior, the data of complaints related to online fraud cases increased by more than 60 percent in 2022.[3]

The frequency of SMS phishing, or "smishing," has been alarmingly rising recently in Cambodian society within increase and more sophisticated.[4] By appearing as an official bank and sending fraudulent SMS messages, scammers deceive their victims.[5] Users are prompted to click on suspicious links in the messages, which take them to a fraudulent website where they are asked to provide personal information.[6] Cambodia Society is being warned, which leads to caution and warning by the Association of Banks in Cambodia.[7]

Unfortunately, the explicit provisions in the Criminal Code of Cambodia 2009 for prosecuting smishing crimes are not outlined in the Criminal Code of Cambodia in specific. However, in the current enforcement, when smishing arises, it fails only under Article 377, which defines "fraud" as something that still lacks some significant offenses that might be relevant. Smishing (SMS and phishing) is a type of phishing that is a form of fraud that uses text messages or short messaging services (SMS) on smartphones and mobile devices to deceive a victim through links that exist in the message.[8]

To accomplish and contribute in order to settle the existing issues, which will explore the following key questions:

1. Should only Article 377, which defines fraud in the Criminal Code of Cambodia, be applied to accusing in smishing crime?
2. What is the difference between the Cambodian Criminal Code and Australia's Criminal Law Framework concerning smishing crime?

By following these questions, this Law Brief article aims to study and explore by understanding smishing crime within Cambodia and Australian jurisdictions, looking at the current legal framework that governs by proposing a measure to address the issues and findings of the study both point out areas for growth in prosecution and add to a comprehensive understanding of the prevention of smishing crime and combating with by comparing Australia jurisdictions.

II. LACK OF PROVISION IN CAMBODIA'S CRIMINAL CODE ADDRESSING SMISHING

Cambodia lacks a specific legal instrument to govern cybercrime, while the amount of cybercrime in Cambodia occurs as noticed. When occurs criminal offenses, only the Criminal Code and some special

[1] Ang Bunnarith, "In 2022 Five major technological crimes committed by criminals digitally," Koh Santepheap, January 03, 2023, https://kohsantepheapdaily.com.kh/article/1662065.html.
[2] Va Sopheanut, "Technology Crimes Are Rising Against Cambodians," Camboja, February 12, 2024, https://khmer.cambojanews.com/cyber-crime-is-happening-more-and-more-on-cambodian-people/.
[3] Long Kimmarita, "Cybercrime complaints up 60% in 2022: official," The Phnom Penh Post, March 16, 2023, https://www.phnompenhpost.com/national/cybercrime-complaints-60-2022-official.
[4] Van Socheata, "Banks warn 'phishing' on rise through mobile apps," The Phnom Penh Post, June 07, 2023 https://www.phnompenhpost.com/national/banks-warn-phishing-rise-through-mobile-apps.
[5] Rov Hongseng, "Warning Issued Over SMS Phishing Scams," KiriPost, June 16, 2023 https://kiripost.com/stories/warning-issued-over-sms-phishing-scams.
[6] Ibid.
[7] Ibid.
[8] Ezer Osei Yeboah-Boateng, Priscilla Mateko Amanor, "Phishing, Smishing & Vishing: An Assessment of Threats against Mobile Devices," Journal of Emerging Trends in Computing and Information Sciences Vol. 5, No. 4 April 2014: pp299s.

laws play a main actor as regulators of society governing which defines offenses, determines those who may be found guilty of committing them, sets penalties, and determines how they shall be enforced.[9]

In terms of smishing, there is only a fraud offense that constitutes to apply for smishing in the criminal code. However, the criminal code itself has some legal provisions that govern offenses related to information technology from articles 427 to 432 that introduce these crimes that are identified as cybercrime.[10] Additionally, the method of smishing seems similar to fraud as well, with a form of deception in which a fraudster disguises himself as an institution, tricked into clicking a link in order to steal our information, which could lead to the loss of any interest.[11] According to Cambodia's Criminal code, article 377 is defined as fraud[12] which this article imposes on perpetrators who involve deceiving an individual or legal person through text messages to obtain funds or property by pretending to be legitimate institutions such as banks or any services by using a fake link or a fictitious capacity in order to impersonate a real position which seems it is trustful which perpetrators commonly aim to trick individual or legal entities to transfer money or disclose financial information through there a fake link in order the perpetrator can access in and transfer money out, in some case perpetrators gain personal information through making document incurring an obligation in there fake platform to the victim which asks to provide financial information or change any financial information that leads to fraudulent and transfers money out.[13] This offense imposes the responsibility for punishable by imprisonment from six months to three years and a fine from one million to six million Riels.[14]

III. AUSTRALIA'S MULTI-CRIMINAL LAW APPROACH TO SMISHING

The majority of scams are deceptive crimes where in Australia, state and federal police look into particular frauds and bring charges against the perpetrators where appropriate, including commonwealth public officials impersonation arrests, fraud-enabling technology arrests, and which include SMS spoofing scam arrests as well.[15] In Australia, cybercrime includes both typical crimes, such as online fraud, where computers or other ICTs are an essential component of the offense, and specifically targeted including denial of service attacks and hacking.[16] Crimes are classified as Commonwealth offenses which fall under the jurisdiction of the Australian federal government. Commonwealth offenses, specifically smishing, are set out in the Criminal Code Act 1995 and under the various State and Territory legislation.[17] Moreover, Prosecution related to Commonwealth fraud may include a broad range of illegal activities, such as phishing-style offenses that impact a Federal government.[18] In addition to addressing the concern of smishing crime, which is a warning to Cambodia and Australian Society, there are laws in Australia that apply variously to smishing crime based on how they use the technical ways and under the various state laws.

1. THE APPLICABILITY OF CRIMINAL CODE 1995 TO SMISHING OFFENSE

Criminal Code Act 1995 is a primary federal criminal law that includes fundamental principles of criminal responsibility for offenses committed inside the Commonwealth outlined in the Criminal Code Act of 1995.[19] Moreover, this code also covers a wide range of cybercrime, including hacking, unauthorized access to computer systems, online fraud, identity theft, etc. In terms of smishing, it falls under section

[9] Criminal Code of Kingdom of Cambodia, Article. 01.
[10] Criminal Code of Kingdom of Cambodia, Article. 427, 428, 429, 430, 431, 432.
[11] GDDTM, "Discover Trick of Phishing and Scam", General Department of Digital Technology and Media, April 12, 2024, https://www.facebook.com/photo/?fbid=853703703450160&set=a.305714791582390.
[12] Criminal Code of Kingdom of Cambodia, Article. 377.
[13] Ibid., Art. 377.
[14] Criminal Code of Kingdom of Cambodia, Article. 378.
[15] Australian Competition & Consumer Commission, "Targeting scams: Report of the ACCC on scams activity 2022,"April 2023: pp27.
[16] CDPP, "Cybercrime," Commonwealth Director of Public Prosecutions, 2024, https://www.cdpp.gov.au/cybercri.
[17] Michelle Makela, "Commonwealth Criminal Offences," gotocourt, October 24, 2022, https://www.gotocourt.com.au/criminal-law/prosecuting-commonwealth-criminal-offences/.
[18] Miralis, Dennis, Jasmina Ceic, and Mohamed Naleemudeen, "Cybersecurity Laws and Regulations Report 2024 Australia," Global Legal Group. November 14, 2023. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia.
[19] Michelle Makela, "Commonwealth Criminal Offences," gotocourt, October 24, 2022, https://www.gotocourt.com.au/criminal-law/prosecuting-commonwealth-criminal-offences/.

478.1.[20] This section imposes the responsibility for the perpetrator who caused unauthorized access or modification to restricted data where the perpetrator accessed restricted data obtained from smishing and used to log into any system intentionally to cause access and knowing that the access was unauthorized. This section prohibited the perpetrator from unauthorized access or modification of restricted data by imposing the penalty of 2 years imprisonment.[21] Moreover, concerning smishing related to possession or control of data with intent to commit a smishing, which constitutes section 478.3.[22] This section imposes liability when the perpetrator obtained the data, such as confidential data, through deceptive methods and can control the data with the intention to use the data to commit other serious computer offenses or facilitate other offenses, which fine a penalty of 3 years imprisonment.[23]

Additionally, in the concern of unauthorized access, modification, or impairment with intent to commit a serious offense, including fraud or identity theft along with smishing, section 477.1 was established to prevent this type of action in smishing methods.[24] This section comes with a maximum imprisonment penalty of 3 years if the perpetrator committed such activities or violated to this section shall constitute under this section.[25]

In the matter of dishonestly obtaining or dealing with personal financial information, section 480.4 shall apply.[26] For instance, in the case of smishing, where the perpetrators use SMS messages to deceive the victim which aims to obtain or to deal with individual financial information by a victim offering personal financial information such as credit card number or bank account information through SMS messages where the perpetrator can access to personal financial information without any consent from a victim whereby victim trust to the message as legitimate message, which this section shall apply and impose imprisonment for five years.[27]

Moreover, concerning smishing, where the perpetrator possesses or controls a thing with the intent to obtain or deal in personal financial information dishonestly, section 480.5 was established to prohibit these actions.[28] When smishing occurs, the perpetrator may possess or control a smartphone, computer, or any computer device used in order to send a deceiving message to the victim and obtain the victim's personal financial information.[29] Furthermore, If the perpetrator intentionally possesses or controls things to send fraudulent messages to obtain personal financial information, it shall apply to this section as well, where this section imposes the responsibility for imprisonment for three years for these actions.[30]

In addition to dealing with the identification information of victims in smishing crimes, section 372.1 was established to charge perpetrators who commit smishing where they deal with the identification information.[31] For instance, smishing crime may involve dealing with the identification information of victims such as name, sex, date of birth, current address, nationality, biometric data, and other information that identifies the victim, while perpetrators may use the identification information to pretend as a victim which leads to perpetrator can access to a bank account or other not legitimacy action for the purpose of committing other offense like fraud or facilitate to other offense for getting benefits where it shall fall under this section which imposes the responsibility for imprisonment for five years for dealing with the identification information of victims.[32] Furthermore, in the case of dealing with money or property that was proceeds of an indictable crime and at the time of the dealing the value of the money or property

[20] Criminal Code Act 1995 of Australia, Section 478.1.
[21] Ibid., Section 478.1.
[22] Criminal Code Act 1995 of Australia, Section 478.3.
[23] Ibid., Section 478.3.
[24] Criminal Code Act 1995 of Australia, Section 471.1.
[25] Ibid., Section 471.1.
[26] Criminal Code Act 1995 of Australia, Section 480.4.
[27] Ibid., Section 480.4.
[28] Criminal Code Act 1995 of Australia, Section 480.5.
[29] Ibid., Section 480.5.
[30] Ibid., Section 480.5.
[31] Criminal Code Act 1995 of Australia, Section 372.1.
[32] Ibid., Section 372.1.

was $1000 or more, it shall fall under section 400.7.[33] Where the perpetrator may deal with money or property obtained through their fraudulent messages, and they may proceed with the value of a property of $1000 or more, which is illegitimacy property from smishing where it shall fall under this section, which imposes the responsibility for imprisonment for five years for these action.[34]

2. CRIMINAL LAW AND SMISHING IN AUSTRALIA

Smishing is a fraud offense involving fraudulent messages where obtaining personal information or financial benefits is unlawful, which shall fall under Australian Criminal Law across all states. In cases where the victim is an individual within the public, charges are filed in accordance with additional State or Territory regulations.[35] Furthermore, when the smishing exists or violates the victim in each state, criminals govern in their territory. For instance, whether smishing offense happens in New South Wales shall fall under Section 192E of the Crimes Act 1900, which defines the definition of fraud constituting a smishing action as well as imposing a maximum penalty of imprisonment for 10 years,[36] in Western Australia, it shall fall under Section 409 of the Criminal Code Act 1913 defines the definition of fraud and imposes a penalty of imprisonment for 7-10years,[37] in Tasmania is shall under Section 253A of the Criminal Code Act 1924 establish the definition of fraud with imposing up to 21-year imprisonment,[38] in Northern Territory it shall fall under Section 227 of the Criminal Code Act 1983 defines the definition of fraud impose punishment 7 years imprisonment;[39] in Queensland it shall fall under Section 408C of the Criminal Code Act 1899 defines the definition of fraud impose a maximum penalty of 5 years,[40] In South Australia it shall fall under Section 139 of the Criminal Law Consolidation Act 1935, which defines the definition of deception impose 10 to 15 year of imprisonment; and in Victoria Section 81 of the Crimes Act 1958 defines obtaining property by deception impose 5 to 10 years of maximum imprisonment.[41] In addition, each state has its specific criminal for charged smishing, which showcases to ensure and protect citizens from deceptive or fraudulent activities such as smishing. Moreover, the imprisonment year ranges from seven to 21 years, depending on the specific situation of smishing activities.

IV. QUESTIONING THE DESIRABILITY OF ADOPTING LEGAL TRANSPLANT FROM AUSTRALIA IN CAMBODIA

In continuation of the discussion above about criminal legal provisions for charging smishing offenses, Cambodia has only one provision for governing smishing, as there is a lack of provision for prosecution. Solely provision exists in Cambodia's criminal code showcasing that lack of understanding in the form of consideration on the action and the method of smishing that it does not involve only deceptive or fraudulent through the message that the perpetrator sends to the victim, which may be raising on concerning about prosecute perpetrator, which is not fulfilled in all of the activities in smishing offense.

However, in Australia, the criminal code and several other state criminal laws have provisions that apply based on all forms of activities of smishing, which include fraud, unauthorized access or modification to restricted data, possession or control of data with intent to commit a smishing, unauthorized access, modification, or impairment with intent to commit a serious offense, dishonestly obtaining or dealing in personal financial information, Possessing or controlling things, dealing with identification information, and dealing with money or property that was the proceeds of an indictable crime, which are demonstrated on the fulfill prosecution to smishing, are unlikely to Cambodia enforcement apply only fraud.

[33] Criminal Code Act 1995 of Australia, Section 400.7.
[34] Ibid., Section 400.7.
[35] Miralis, Dennis, Jasmina Ceic, and Mohamed Naleemudeen, "Cybersecurity Laws and Regulations Report 2024 Australia," Global Legal Group. November 14, 2023. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia.
[36] Crime Act 1900 of New South Wales, Section 192E.
[37] Criminal Code Act Compilation 1913 of Western Australia, Section 409.
[38] Criminal Code Act 1924 of Tasmania, Section 253A.
[39] Criminal Code Act 1983 of Northern Territory, Section 227.
[40] Criminal Code Act 1899 of Queensland, Section 408C.
[41] Crimes Act 1958 of Victoria, Section 81.

In the present case in New South Wales, a man has been detained by the AFP police on suspicion of operating out of Sydney to obtain the financial and identity information of thousands of Australians in order to get access to their accounts. He was arrested and charged with seven offenses according to the criminal code and other state criminal laws.[42]

In addition to the present case in Cambodia, the new scam to telegram users by sending a fraudulent link to SMS message for telegram users to access the link and fill in the information and scam money under the guise of exchanging money to pay for goods and transfer money through a bank to proceed in investigating the case of fraud as shown above in the amount of $ 143,560 Until the arrest of a male suspect, the police sent the suspect and charged him with a fraud offense.[43] The case report shows that Cambodia's prosecution still needs to fulfill all relevant activities due to the lack of provisions to address the smishing offense.

V. CONCLUSION

In conclusion, this law brief shows that Cambodia and Australia highlight important gaps in Cambodia's Legal framework for addressing smishing that only based on general fraud provisions, which is why this approach is insufficient to address the difficulty of smishing. While currently smishing, waring society involves various fraudulent practices. Unlike the Australian legal framework, which consists of both federal and state laws, it provides a mechanism for prosecuting smishing by concerning different aspects.

In order to strengthen the prosecution and combat smishing in Cambodia, developing and reforming the specific legal provisions that cover various smishing activities and involve cybercrime is vital. Learning from Australian efforts and the multi-criminal law framework approach, Cambodia should follow Australia's enforcement by enhancing its legal instruments, specifically the Cambodian Criminal Code, to include more provisions relevant to smishing action for the prosecution enforcement mechanisms for smishing and related cyber offenses as well.

[42] Australian Federal Police, "Second Man Charged over SMS Phishing Scam," AFP Media, August 11, 2022, https://www.afp.gov.au/news-centre/media-release/second-man-charged-over-sms-phishing-scam.
[43] KC Virak, "Technology Crime Department bans clicking Telegram link scam," Kampuchea Thmey Daily, 23 May 2023, https://www.kampucheathmey.com/security/515356.

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

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

9 789924 571278