KONRAD ADENAUER STIFTUNG

THE LAW TALK PUBLICATION

REGULATING PERSONAL DATA PROTECTION AND CYBERSECURITY

PRACTICAL AND LEGAL CONSIDERATIONS FOR CAMBODIA AND BEYOND

KONRAD ADENAUER STIFTUNG

ABOUT KONRAD-ADENAUER-STIFTUNG

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

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

ABOUT ROYAL UNIVERSITY OF LAW AND ECONOMICS

The Royal University of Law and Economics (RULE) is the first and oldest higher education institution in Cambodia. It was originally founded in 1949 as the "National Institute of Law and Economics". RULE maintains its position as the first and leading national university in the area of Law, Public Administration, International Relations, Accounting, Banking and Finance, Economics and Management. RULE has around 15,000 students with four faculties: Law, Public Administration, Economics and Management, and Informatic Economics.

In accordance with the Education Strategic Plan and Higher Education Vision 2030 from the Cambodian Ministry of Education, Youth and Sports, RULE has set its own strategic plan following the vision that will guide the university's journey from 2015 through 2018 to respond to the emerging labor market. The mandate of RULE is to ensure the quality of education, innovation, research and publication. RULE has broadly expanded its international collaboration with many qualified foreign universities to promote academic exchange. RULE currently has international agreements with 19 foreign universities and research institutions and is one of the two Cambodian higher education institution members of the ASEAN Universities Network.

ABOUT NATIONAL UNIVERSITY OF MANAGEMENT

Throughout the course of 39 years, the National University of Management has been developing progressively in terms of capacity, diversity, and quality education, based on our core values of research, entrepreneurship, and innovation, which take our students and alumni to brigher future.

The National University of Management is firmly committed to the development of competent and socially responsible human resources with high intellectual knowledge, skills, and ethics in order to be able to make more productive contribution to the socio-economic development of the country.

ABOUT LAW TALK

Since 2006, Konrad-Adenauer-Stiftung (KAS) Cambodia and our partners have hosted The Law Talk every year as part of our ceaseless effort to advance a culture of legal academic work and legal discourse in Cambodia and the region. Individuals with diverse backgrounds in law, including academics, researchers, scholars, students, public officers, politicians, NGO workers, embassies, and international organisations, are invited to participate in a meeting to discuss specific legal issues. Every law talk that has taken place over the years has covered a wide range of legal subjects, such as criminal law, labour law, human rights, environmental law, constitutional law, law pertaining to political parties, law pertaining to consumer protection, and so forth.

Partners that we have previously collaborated with include the Senate, the National Assembly, the Cambodian Constitutional Council, and relevant ministries in Cambodia.

At the 22nd Law Talk, which was held on November 30, 2023, up to 60 legal scholars and practitioners from Cambodia and overseas were invited to participate in and shape the discussion surrounding the legal development of “Cybersecurity and Data Protection in Cambodia and Beyond.”

Under the framework of Law Talk Publication, co-organised by KAS, the National University of Management (NUM), and the Royal University of Law and Economics (RULE), a number of scholars from Cambodia and abroad have contributed chapters covering various subtopics associated with the theme mentioned above. As the host, KAS Cambodia commits to carrying on the delivery and facilitation of the dialogue on legal issues affecting Cambodia and the region around it.

Publisher Information

'Regulating Personal Data Protection and Cybersecurity: Practical and Legal Considerations for Cambodia and Beyond' is published by the Konrad-Adenauer-Stiftung Cambodia.

Editors:
Kong Phallack
Thomas Honnet

ISBN 978-9924-571-25-4

The Law Talk Publication

REGULATING PERSONAL DATA PROTECTION AND CYBERSECURITY

PRACTICAL AND LEGAL CONSIDERATIONS FOR CAMBODIA AND BEYOND

Content

FOREWORD

The Country Director of KAS Cambodia

As Cambodia navigates the complexities of an increasingly digital world, the importance of robust legal frameworks to protect data, ensure cybersecurity, and promote responsible technology use cannot be overstated. This year's Law Talk publication, brought to you by the Konrad Adenauer Stiftung in Cambodia, delves into these critical issues, offering a comprehensive exploration of the challenges and opportunities that lie ahead.

The theme of data protection is central to this publication, reflecting the growing concerns over privacy and the safeguarding of personal information in an increasingly digital world. This publication explores various facets of this issue, from the protection of children's data to the broader regulatory frameworks that govern data processing. A comparative analysis of international laws, particularly the European Union's General Data Protection Regulation (GDPR), provides valuable insights into how different jurisdictions are tackling these challenges and offers lessons for Cambodia as it continues to develop its own legal frameworks. The comparison with Vietnam's recent personal data protection regulations, for example, offers valuable lessons that could inform Cambodia's own legislative efforts.

Cybersecurity is another critical area examined in this volume. The growing threat of cybercrime, as highlighted in discussions on criminal liability for legal persons, underscores the need for robust regulatory mechanisms. By examining the approaches taken by the European Union and the United States, this publication identifies key principles that can guide the development of effective cybersecurity laws in Cambodia, while delving into the complex issue of cross-border data flow, which has become increasingly relevant in today's interconnected global economy.

We extend our deepest gratitude to all the authors, legal scholars, and practitioners who contributed to this publication. Their expertise and insights are invaluable as Cambodia navigates the complex legal challenges of the digital age. We also thank our partners and supporters who have made this publication possible.

We hope that this edition of the Law Talk will not only inform but also inspire readers to engage in the ongoing discourse on these critical issues. The need for continued discussion and collaboration is more urgent than ever, and we look forward to seeing how these conversations will shape the future of law and policy in Cambodia.

Jason Chumtong
Country Director
KAS Cambodia

FOREWORD

The Rector of the National University of Management

It is with great pleasure that I introduce this Law Talk publication, titled "Regulating Personal Data Protection and Cybersecurity," a collection of insightful essays authored by both Cambodian and international scholars. This timely work explores the complex landscape of personal data protection and cybersecurity, areas of growing importance in our increasingly digital world. As our society becomes more connected, the need to safeguard personal information and ensure robust cybersecurity measures has never been more critical.

This publication is more than just a compilation of legal perspectives; it is a testament to the collaborative efforts of experts dedicated to shaping the future of law and policy in Cambodia. The diversity of viewpoints presented here not only enriches our understanding but also offers practical guidance for developing comprehensive legal frameworks that address the unique challenges faced by our nation.
At the National University of Management, we recognize the vital role that research and innovation play in addressing the most pressing issues of our time. The insights offered in policy articles are invaluable to policymakers, legal practitioners, academics, and all those engaged in the crucial work of national development.

I would also like to extend our deepest gratitude to the Konrad-Adenauer-Stiftung (K.A.S.) for their generous support in covering the publication cost of this book. Their commitment to promoting informed dialogue and policy development in Cambodia is greatly appreciated and has made this important work possible.
I extend my sincere thanks to the authors and contributors for their dedication. I trust that this book will inspire further research and collaboration, helping to shape a safer digital future.

H.E Dr. Hor Peng
Rector
National University of Management

MESSAGE FROM CO-EDITORS

The digital revolution is over since technology reshapes every aspect of life and transform how we live, work, and think. Technology is rewriting the rules, makes the world shrinks, national boundaries blur, and cultural differences intertwine. To thrive in this new reality, countries must adapt to standardized global rules governing trade, data protection, cybersecurity, and fundamental freedoms. We believe the Kingdom of Cambodia, a small nation state with limited resources on technologies development and innovation, is part of this context. The kingdom is facing the difficult balance between respect for major international principles and the preservation of national specificities, between the internationalization of legal rules and the protection of local particularities.

As co-editors, we are pleased to present a Law Talk Publication titled Regulating Personal Data Protection and Cybersecurity. Through this publication, we aim to contribute to the ongoing dialogue and provide insights that can inform policy development, business strategies, and legal practices.
This book is a small stone on this long road. It brings together a diverse range of perspectives from scholars on data privacy and cybersecurity in today's digital landscape. We would like to extend our deepest gratitude to all authors whose expertise and dedication have made this work possible. We also thank the National University of Management, the Royal University of Law and Economics and KAS Cambodia for their support in bringing this project to fruition.

As co-editors, it is our hope that this book will serve as a valuable resource for professors, students, professionals, and decision-makers alike to deep dive researches, discussions, and innovation in the fields of data protection and cybersecurity.

Kong Phallack & Thomas Honnet

EXECUTIVE SUMMARY

The Law Talk Publication: Regulating Personal Data Protection and Cybersecurity

The Law Talk Publication , **"Regulating Personal Data Protection and Cybersecurity"** presents two critical areas shaping the digital landscape personal data protection and cybersecurity. The regulation of these domains has become essential to safeguarding privacy, national security, and the integrity of global digital infrastructure in this digital age. This book aims to provide a entry point for professors, students, professionals, and decision-makers alike to deep dive researches, discussions, and innovation in the fields of data protection and cybersecurity. It is divided into two parts and 11 chapters. Part 1 discusses about Personal Data Protection and Part 2 delves into cybersecurity. Below is topics covered in each chapter, providing summary for readers and guidance on the focus and key takeaways of the articles.

PART 1: PERSONAL DATA PROTECTION

Chapter 1: Developing a Comprehensive Personal Data Protection Framework for Cambodia. This paper explains the ideas and processes of development of personal data protection in Cambodia, the envisioned personal data protection governance, the implementation regulations and plan when the law on personal data protection is promulgated and entry into force.

Chapter 2: Cross-Border Data Flow - An Appropriate Approach and Mechanisms for Cambodia. This paper contributes to scholarly discourse on cross-border data flow, explore the mechanisms facilitating data transfer, and formulate an appropriate policy framework to govern cross-border data flow in Cambodia.

Chapter 3: Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia This article examines legal trends and cases from the European Union and recommend policies for Cambodia to adopt to address privacy and data protection issues that may arise in competition.

Chapter 4: Blockchain Technology and Personal Data Protection for Cambodia: Personal Data, Data Controller, and Right to Be Forgotten. This article explores the challenges posed by blockchain technology to personal data protection principles in the General Data Protection Regulation. The discussion shows how blockchain's features could potentially undermine conventional data protection paradigms with regard to personal data, data controller, and "right to be forgotten".

Chapter 5: The GDPR and the Vietnamese Decree n°13/2023/ND-CP: Comparative Analysis of a Recent Legal Framework in Southeast Asia Regarding the Personal Data Protection. This chapter provide a comparative analysis of between GDPR and the Vietnamese Decree n°13/2023/ND-CP, and to draw out the good and bad ideas, so that Cambodia will not make the same mistakes and will find its own way.

Chapter 6: The Influence of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data on the GDPR. This article explains the history and influence on the Convention 108 on the development of GDPR.

Chapter 7: A Though on Child's Best Interest in Data Protection. This article intends to assess different data protection frameworks in the attempt and approaches to protecting child's data and privacy rights. This paper is written in cognizance of the ever-growing presence of children online and the increased processing of children data both on and offline.

PART 2: CYBERSECURITY

Chapter 8: Designing a Cybersecurity Legal Framework for Cambodia. This paper explains the ideas and processes of development of cybersecurity law in Cambodia, the envisioned cybersecurity governance, the implementation regulations and plan when the law on cybersecurity is promulgated and entry into force.

Chapter 9: Digital Security in the European Union – Regulations and the Future of Digital Security and Resilience. This article explains the digital security regulations in the European Union by selecting specific regulations and experiences of EU. The article suggests for Cambodia to push for greater cooperation in cyber security within the Association of Southeast Asian Nations (ASEAN).

Chapter 10: Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law. This chapter provide approaches taken by US and EU in creating cybersecurity regulatory mechanism.

Chapter 11: Criminal Liability of Legal Person in cybercrime. This paper takes into account the foreign norms as bench mark for thinking to identify gaps in Cambodian laws related to criminal liability of legal persons for cybercrime with possible recommendations.

ABOUT THE AUTHORS

Professor Kong Phallack

Prof. KONG Phallack is a long-standing legal professional with over two decades of experience in teaching, policy development, legal practice, arbitration, and mediation. He holds a Master of Laws (LL.M.) from Nagoya University in Japan, a Bachelor of Laws (LL.B.) from Royal University of Law and Economics, and a Doctor of Dental Surgery (DDS) from Royal University of Health Sciences. Prof. Phallack had served as a dean the Faculty of Law and Public Affairs of Paññāsāstra University of Cambodia until 2020. His academic career includes adjunct and visiting professor roles at several domestical and foreign universities.

His publication includes Introduction to Cambodian Law (2012), Cambodian Constitutional Law (2016), Contemporary Environmental Law in Cambodia and Future Perspectives (2020), Perspectives on Cambodian Constitutional Law (2020), Contemporary Cambodian Employment and Labor Law (2021), and Law in the Digital Age: and Protection of Consumer Rights (2021). His previous contribution to development of laws and policies are legal and judicial reform, alternative dispute resolution, ombudsman and local compliant dispute resolution, civil code and procedures, labor mediation and arbitration, labor and employment, legal aid, public private partnership, social protection, social security, persons with disabilities, environment, water, energy, health, A2I and so on.

Currently serving as the Secretary of State of the Ministry of Post and Telecommunications, Prof. Phallack leads the Legal Team responsible for developing legislation in the digital and postal sectors including telecommunication infrastructure sharing, radio frequency spectrum management, QoS, Domain Name .kh, Verify.gov.kh cybersecurity, personal data protection, digital transformation, digital government. His going-on research, policies and legislation development includes ICT, internet governance, data governance, open data, cloud computing, Artificial Intelligence, telecommunication submarine cable, satellite communication, and application of international law in cyberspace.

Sous Monirida

Sous Monirida is an accomplished legal professional with a compelling academic background. She was honored with the RWI scholarship for her bachelor's degree in law from the esteemed Royal University of Law and Economics. Pursuing her passion for knowledge and growth, Monirida Sous pursued a master's degree in Japan, broadening her expertise and global perspective. Currently, she is serving in a governmental institution by actively contributing to the drafting of laws and regulations aimed at driving sectoral development. Additionally, she also extends the horizon of a professional career in educational fields at one prominent university in Cambodia on intellectual property law subject. Her commitment to research is evidenced by her publication on consumer protection with Konrad Adenauer Stiftung. With research interests spanning intellectual property, consumer protection, telecommunications, and digital-related law and policy, Monirida Sous remains at the forefront of legal developments, driven by her desire to make meaningful contributions and create a positive impact on society.

Keo Sothie

Keo Sothie serves as Secretary of State of the Ministry of Post and Telecommunications. In his role, he oversees the legal work of the Ministry including legislation drafting, arbitration and litigation, and contracts. He has recently helped spearhead the drafting of key laws, regulations, and policies including the Cybersecurity Draft Law, Personal Data Protection Draft Law, Postal Sector Draft Law, Digital Sector Management Draft Law, and Cloud First Draft Policy. With the adoption of the Digital Economy and Society Policy Framework 2021-2035 and Digital Government Policy 2022-2035, the Royal Government of Cambodia is on a rapid path toward digital transformation. Mr. KEO is also a member of the Secretariat of the National Digital Economic and Social Council, established from the Digital Economy and Society Policy Framework 2021-2035. Mr. KEO is a licensed lawyer both in the Kingdom of Cambodia and the State of Colorado. He received his Juris Doctor and Master of Laws from Northwestern University School of Law and a Bachelor of Arts in Political Science from the University of Washington. During his spare time, he teaches law at the American University of Phnom Penh as an Adjunct Law Professor. He is married and has one daughter.

Ros Sophearathna

Ros Sophearathna is a legal officer at the Ministry of Post and Telecommunications. She engages in legal research, training, negotiations, and legislation drafting on various laws, regulations, and policies such as Cybersecurity, Personal Data Protection, Competition, and consumer protection. She received two Bachelor of Arts in Law from both the American University of Phnom Penh and the University of Arizona. She is currently pursuing a master of Law at the American University of Phnom Penh and a master in Public International Law at the Royal University of Law and Economics.

Phan Daro

Phan Daro leads the Center for Digital Governance and Technology Promotion of the Institute of Digital Governance under the Cambodia Academy of Digital Technology and is an adjunct lecturer at the Faculty of Law and Public Affairs and the Faculty of Education of PaññāsāstraUniversity of Cambodia. Prior to this, Daro worked as an official in the appeal section of the Administrative Office at the Phnom Penh Municipal Court. He holds bachelor's degrees in education, computer science, and law before receiving his LL.M. from Nagoya University, Japan. He is currently working on blockchain governance, information technology law, cybersecurity policy, and intellectual property rights. His previous works include Digital Infrastructure in Cambodia: The Current Status and BudgetExpenditures (Transparency International Cambodia, 2022), Copyright Interests during Employment: Some Guidance for Decision-Making (FLPA and Solidarity Center, 2021); The Apparent Transfer of Environmentally Sound Technologies to Cambodia(Konrad-Adenauer-Stiftung, 2020); Protecting Geographically Indicative Goods of Cambodian Farmers(Faculty of Integrated Social Sciences, Khon Kaen University, Nongkhai Campus, 2019); Legislative Supports for The Collective Management of Copyright and Related Rights in Cambodia (GSL, Nagoya University, 2017); Copyright Protection for Computer Programs in Cambodia (RULE, 2014) (in Khmer). He also co-edits the second edition of Contemporary Cambodian Labor and Employment Law: Digital Economy and Post-pandemic Society (FLPA and Solidarity Center, 2022).

Thomas Honnet

Graduated from La Sorbonne law school 10 years ago with a Master 2 in digital law, Thomas Honnet is currently an expert in personal data protection. After working at the French National Assembly then in a law firm, he then worked with Ministries in France on their GDPR compliance. He also supported Vietnam in setting up their eGovernment, with an international support mission. Today, he is the Data Protection Officer of the City of Marseille, France's second largest city. For the past 10 years, he has been teaching at various prestigious schools and universities (Sciences Po, Sorbonne, Assas) and regularly taking part in conferences and seminars on digital law, as he is convinced that digital law needs to be thought through before it can be applied.

Federico Ferretti

Prof. Ferretti Federico, Associate Professor in Economic and Financial Markets Law, Department of Sociology and Economic Law, University of Bologna (Italy). Jean Monnet Chair of Digital Market Law (2022-present) funded by the European Union. Director of the Jean Monnet Centre of Excellence"Consumers and SMEs in the Digital Single Market" ('Digi-ConSME') funded by the European Union (2019-2023). Qualified Lawyer of the High Courts of Italy. Formerly, Senior Lecturer in Law at the University of London (UK). Member of the Consumer Advisory Group (CPAG) of the European Commission. Member of the Financial Services User Group (FSUG) of the European Commission. He advises in the preparation of legislation or policy initiatives which affect consumers and the users of financial services, providing insight, opinion and advice concerning the practical implementation of consumer policies. As a practitioner, he served as the lawyer of a multinational company providing credit data and scoring services internationally. He also advised regularly national and European consumer interest groups. He held various visiting positions in several countries. From the academic year 2023, he is a visiting professor at the Royal University of Law and Economics (Phnom Penh, Cambodia) teaching the module 'Data Protection Law'.

Dr. Patricia Boshe

Dr. Patricia Boshe is a data privacy trainer and consultant. She is a co-founder and co-director of the African Law and Technology Institute (AFRILTI); a research institute focusing on the interrelation between law, technology and society from an interdisciplinary perspective. She has more than 10 years' experience as a law lecturer in Tanzania. Currently, a senior researcher at the Research Center of Law and Digitalisation at the University of Passauin Germany. Some of her research activities involve assessments and critiques on privacy and data protection in Africa. Her publication record includes a book on data protection, book chapters and over dozen of international referred journal articles, book reviews, and practical legal comments.

Ferdinand Gehringer

Ferdinand Gehringer has been working at the Konrad-Adenauer-Stiftung since March 2021 and since November 2021 as a Policy Advisor for Cybersecurity in the Department of International Politics and Security. Prior to that, he initially worked as a Policy Advisor for International Law and Rule of Law and he was the Coordinator of the Foundation's Rule of Law Programmes. Ferdinand Gehringer is a licensed lawyer and certified mediator. He studied law at the Johannes Gutenberg University in Mainz and at the Universidad de Valencia (Spain). After gaining professional experience at the law firm Hengeler Mueller in commercial law, at the European Parliament in Strasbourg and Brussels and at Roedl & Partner Abogados y Asesores in Barcelona, he completed his studies with the first state law examination in Mainz. During his legal clerkship at the Higher Regional Court of Frankfurt am Main, he worked, among others, for the Federal Supervisory Authority for Air Traffic Control in Langen, the GermanMinistry of Foreign Affairs at the German Embassy in Yerevan (Armenia), the law firm Taylor Wessing in construction and real estate law and for the Rule of Law Program Latin America (Colombia) of theKonrad-Adenauer-Stitung, before he completed his clerkship with the secondstate law examination.

Dr. Meas Bora

Dr. Meas Bora got both a Master's and Doctoral Degree in Law from Nagoya University Graduate School of Law, Japan, after graduation from the Faculty of Law and Economic Sciences in 1998, Phnom Penh. He obtained the United Nations International Law Fellowship Program to study international law at The Hague Academy of International Law, the Netherlands, in 2011. In 2015, he was a visiting researcher at the Centre for Asian Legal Exchange in Japan on Criminal Liability of Legal Person.

He is the president of the Cambodian University for Specialties (CUS) since October 2018. He has given lectures on international law, human rights, international criminal justice to the universities and the Bar Association of the Kingdom of Cambodia. He wrote several articles in English on extradition, human rights, criminal procedure, the rights of the accused, and one book in Khmer on introduction to public international law. He was a legal team leader of the Office of the Co-Investigating Judges of the Extraordinary Chambers in the Courts of Cambodia (ECCC). Since 2015, he is a member of the Council of Jurists of the Council of Ministers, Royal Government of Cambodia and in 2018, was appointed as one of the members of the National Committee of Cambodia ASEAN Law Association (ALA).

He was admitted to the Bar Association of the Kingdom of Cambodia in 2012 and 2017 as a vice-chair of the international law and human rights commission thereof. Before this, he was a consultant for UNICEF in Cambodia on the edition of the draft report on the implementation by the Kingdom of Cambodia of the Convention on the Rights of the Child, and for the Cambodian National Council for Children on Analysis of Legal Framework for the Protection of Children in Cambodia.

PART I
PERSONAL DATA PROTECTION

Personal Data Protection

Developing a Comprehensive Personal Data Protection Framework for Cambodia

Professor Kong Phallack

Abstract

The Constitution of Cambodia recognizes the right to privacy and human rights enshrined in the UN Charter, International treaties, conventions and agreements ratified by Cambodia.[1] Article 12 of the Universal Declaration of Human Rights (UDHR) state "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.... Everyone has the right to protection by the law against such interference or attacks." Furthermore, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) recognizes the need for adoption of personal data protection to safeguard the right to privacy. Cambodia government has taken into consideration the need of data privacy and protection law and determine the formulation of this law in the Cambodia government introduced the Digital Economy and Society Policy Framework 2021-2035 (DESPF)[2], Cambodia Digital Government Policy 2022-2035 (CDGC)[3]. Therefore, this paper is prepared to explain the development of draft law on personal data protection in Cambodia.

Introduction

Personal data protection legislation is a MUST in digital age since increasing of online activities of citizens, businesses and governments, and expansion information technology capabilities. Data can be searched, edited and shared with each other across the globe; and the processing of personal data becomes widespread in particular in the era of emerging AI technology, adaption and use. "Human needs food whereas AI system needs data including personal data". Data is the foundation for AI. Processing of personal data by AI system can lead to violation of privacy, for instance, unauthorized access, data breach, profiling and misuse of personal information especially sensitive information of individual.

Despite absence of personal data protection law, currently there are number of laws and regulations having provisions related to Personal Data Protection Constitution, Civil Code, Law on Telecommunications, Law on E-Commerce, Sub-decree No.110 ANKr.BK on Licensing of ICT operation (Sub-decree No.10) etc. According to sub-decree No.110, ICT operators have obligations to protect privacy, security and safety of usage of ICT services.[4] However, Cambodia needs a comprehensive personal data protection legal framework in to order to promote the development of Cambodian digital economy. The DESPF and the CDGC entrust the Ministry of Post and Telecommunications (MPTC). On 9 September 2021, the Ministry of Post and Telecommunications (MPTC) established a working group on drafting Law on Personal Data Protection. This working group is tasked to prepare the Draft Law on Personal Data Protection (PDPL), research on Laws and polies related personal data Protection in the region and the world, cooperate with relevant ministries and stakeholders in order to ensure the PDPL is in-line with national and international legal instruments. Thus, the below section explains the key provision of the PDPL in Cambodia.

Designing the Draft Law on Personal Data Protection in Cambodia

This section explains the development of personal data protection law in Cambodia and key provisions of the draft law. It is a personal opinion of the author. It neither represents the position of the Working Group of PDPL nor the Ministry of Post and Telecommunications.

1 Cambodia Constitution (1993), Art.31, Art. 40
2 Digital Economy and Society Policy Framework 2021-2035 (DESPF, Policy Measure No.34, p.73
3 Cambodia Digital Government Policy 2022-2035 (CDGC), Priority Action No.20, p.39
4 Sub-decree No.110 ANKr.BK on Licensing of ICT operation (Sub-decree No.10), Article 27 (f)

As mentioned above, the DESPF and the CDGC directs the development of laws and policies related to Data protection and Privacy[5] and personal data protection law. The two policies are basis for consideration of the development of the Cambodia's PDPL. Furthermore, the relevant laws and regulations enforced in Cambodia, Laws, policies, strategies, reports, research papers related to personal data protection such as UNDP, UNESCO, UNCTAD, ASEAN, APEC, EU and selected countries such as Estonia, Singapore, Japan, Australia, Thailand, Vietnam, Malaysia, USA, Canada, China, South Korea, etc. are also reviewed and consulted. The PDPL was circulated for inputs from stakeholders such as local and foreign companies, business associations, embassies as well as international organizations based in Cambodia. At the time of writing, the PDPL is being reviewed and consolidate inputs from stakeholders.

Purpose and Scope of the Draft Law on Personal Data Protection

Personal data under the PDPL means any information relating to an identified or identifiable natural person which is known as a data subject. Examples of personal data include a name, a home address, an email address, an identification card number, location data - an Internet IP address, a cookie ID, phone number, data held by a hospital or doctor, or professionals etc. The identifiable natural person is the one who can be identified directly and indirectly in particular by reference to a name, identification number, location data, online identity or more identifiers related to physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

The PDPL is developed with the purpose to i) promote the protection of rights of data subjects by balancing with the interests of entities in carrying out their functions or activities; ii) enhance responsible and transparent personal data processing, iii) facilitate the cross-border data transfer with while ensuring that the rights of data subjects are respected, and iv) contribute to create new industry in the era of digital economy and society.

The PDPL applies only to the processing of personal data by automated means by data controllers located in the Kingdom of Cambodia and data controllers resided outside Cambodia but their business activities for the data subjects in Cambodia. The data controller in the PDPL refers to a natural person, private legal entity, public administrative establishment and public enterprises because the approach taken in the PDPL is to have two separate pieces of Legislation for one for government and one for the private. other public authorities such as ministries and institutions process personal data are governed by a separate regulation.

The PDPL does not apply to processing personal data that is publicly available, processing personal data for domestic or household purposes, national sovereignty, national security, defense, public interest, public health, crime prevention and investigation, etc. Detail rules and guidelines one exemptions are determined in the Common Guidelines for Personal Data Protection or separate regulations.

The Governmental Entities in Charge of Personal Data Protection

The PDPL empowers the Ministry of Post and Telecommunications as a regulatory authority and it is empowered to lead, manage, monitor, and oversee personal data protection in the Kingdom of Cambodia. A Unit in charge of Personal Data Protection will be created and functions as a secretariat to Ministry of Post and Telecommunications.
The organization and functioning of the Unit in charge of Personal Data Protection is determined

5 Ibid 1, pp. 70-75

by Sub-Decree upon the proposal of the Minister of Ministry of Post and Telecommunications. Several models of Unit in charge of Personal Data Protection are reviewed. Those models include GDPR's suggested Model, Thailand's Personal Data Protection Committee, Singapore's Personal Data Protection Commission, Japan's Personal Information Protection Commission, Australian Information Commissioner, and the Philippines' National Privacy Commission etc.

Processing of Personal Data

The PDPL states that the processing of personal data shall comply with principles and legal basis set in the law. The data controller or processor must identify the legal basis by which their processing of personal data is permitted. Processing as defined in the PDPL, it refers to the entire lifecycle of data such as collection, recording, organization, storage, alteration, retrieval, use, disclosure by transmission, dissemination, erasure, and destruction.

The PDPL sets principles and legal basis for processing of personal data. The principles include i) lawfulness, fairness and transparency; ii) purpose limitation; iii) data minimization; iii) accuracy; iv) storage limitation; vi) integrity and confidentiality; and vii) accountability. These principles form as the basis for processing personal data. Whereas the legal basis, the idea is that data controller processes personal must comply with one of six legal requirements such as i) consent (for one or more specific purposes), ii) necessity for performance of contract or at the request of data subject prior to entering into a contract, iii) necessity for data controller to comply with a legal obligation, iv) necessity to protect the vital interests of the data subject or of another natural person, v) necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and vi) necessity for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The PDPL determines also conditions for processing of special category of personal data such as a child data and sensitive data. Processing personal data of a child below 16 years old requires consent from parents of guardian for. As for the processing of sensitive personal data, the PDPL provides a broad category of sensitive data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The detail conditions, formalities and procedures of processing personal data are determined by the Common Guidelines for Personal Data Protection.

Rights of Data Subject

Like Personal data protection law in other countries, the PDPL in Cambodia provides the rights of data subject which include:

Right to be informed that means data subjects must be provided with information about how their personal data is being processed by the data controller whether it is direct processing or indirect processing. The data controller must be able to explain the source of the data;

Right to access that means data subjects must be able to obtain information about the collection, storage, or use of their personal data. The information should include a confirmation of processing by a data controller, the purpose of processing, the legal basis for processing, sources of obtaining personal data, information related to personal data sharing and storing and data is being used for profiling and automated decision-making;

Right to rectification that means data subjects have the rights to request the data controller to correct, update or modify their data if the is inaccurate, erroneous or misleading;

Right to erasure that means data subject have the rights to request data controller to erase his or her personal data, to stop dissemination or sharing, etc. However, the exercise of right will be taken into account the public interest of keeping data remaining and right of data subject;

Right to restrict processing that means the data subjects have the right to restrict or block or suppress processing personal data until issues between them and the data controller are solved; Right to data portability that means the data subjects have the rights to request the data controller to make their personal data processed by data controller be available in the universally machine-readable format or transmitted to other services with their consent;

Right to object that means the data subjects have the rights to object their personal data being processed anytime and the data controller must provide evidence and reasons why their personal data must be continued to be processing. The justification of continuing processing must be obvious and have greater benefits than respecting the rights of the data subjects;

Rights about automated decision making and profiling that means the additional right given to data subjects in relation to automated decision making and profiling. The Automated decision making means the new way of processing personal data by using technology. The automated decision can lead to in accurate, unfair or discriminatory decision because it relies on machine and technology. Profiling means that facts that the processing of personal data can be derived, inferred and predicted from other data sources such as advertising, healthcare, etc.. is qualified as a processing of personal data, and the data subject shall be informed about their rights and how they exercise the rights of data subject in the context of Automated decision making and profiling; and

Right to complaint and remedy that means data subjects have the rights to lodge a complaint against data controller for non-compliance the law on personal data protection and get any forms of remedies or compensation and that data controller shall be accountable for their non-compliance.

As explained above, the idea behind rights of data subjects is to impose obligations on data controllers regarding processing of personal data and this right will be enforceable before the Unit in charge of Personal Data Protection and the competent courts of the Kingdom of Cambodia. However, such an obligation is exempted as explained in section of scope of PDPL.

Data Controller and Data Processor

The PDPL requires data controller and data processor to comply with obligations established in the law by taking necessary measures to protect personal data processing by them during the life cycle of personal data. The relationship between data controller and data processes is bound by the contract. The DPDL defines data processor is a person processes personal data on behalf of a data controller. That means burden on data processor include Obligations specifically written in the contract and obligations provided by the law. Therefore, the data processor is obliged to implement appropriate technical and organization measure to protection personal data on behalf of the data controller.

As a general rules, both data controller and data processor are obliged to fulfill these obligations but not limited to *i) employ or appoint a qualified a data protection officer (s) to oversee the processing of personal data; ii) Develop and adopt Internal Regulations on Personal Data Protection; iii) adopt the*

both protection by design and protection by default approach; iv) conduct personal data protection impact assessment; v) implement PDPL measure of data and infrastructure and device used at every stage of processing personal data from general processing activities to collection, retention and sharing; vi) report and investigation of data breach and inform the Unit in charge of Personal Data Protection, relevant authorities and the affected data subject.

The DPDL include the concept of technology means used in designing the system of protection with the aim to protect the privacy of data subject and their rights of provided by the PDPL. The technology means used in designing the system of protection in this article is referred to the data protection by design and data protection by default.

The data protection by design requires data controller and data processor to take into consideration of data protection from the designing stage of the system in order to reduce reliance on obligations imposed by the law. This approach is called "Protection of Personal Data by Technology itself" which means embedding privacy concept into design and architecture of systems, services and business practice from outset to ensure full lifecycle protection. Data Protection by Design or Privacy by design is vital for protection of personal data this concept is called proactive approach rather than active approach.

The data protection by default requires data controller and data processor to take into consideration in applying data protection by default concept in the system, products or services without any inputs from the end users. This concept reduces or removes burden on users or data subjects having superficial knowledge and do not understand the complexity of technologies, systems, products or services. Therefore, they systems and applications should come with security setting at highest level such as encryption; authentication; automatic protection measures such as firewalls, intrusion detection, and malware protection; and systems updated such as security and patches to address vulnerabilities.

In a nut shell, despite explaining in this article, detail requirements of obligations of data controller and data processors are to be regulated in the Common Guidelines for Personal Data Protection.

Data Storage and International Data Transfer

The PDPL requires the data controller to store collected personal data in the Kingdom of Cambodia. A data controller may choose to store collected personal data in its own personal data storage system or a national data center, data centers operated by licensed ICT operators or a secured cloud system of a third party licensed by MPTC in accordance with other laws and regulations in force. Whereas the international transfer of personal data is required an authorization by provisions of the law and regulations. Different models have been reviewed, in the particular EU Model of assessment of the adequacy of protection mechanisms of personal data by the recipients of personal data such as laws of the recipient countries biding corporate rules and so on.

As explained in the purpose of the law, the DPDL aim to facilitate the cross-border data transfer with while ensuring that the rights of data subjects are respected, and contribute to create new industry in the era of digital economy and society. Since Cambodia is a member of ASEAN, Cambodia will consider the alignment of its personal data protection rules to ASEAN Framework on Personal Data Protection (2016), ASEAN Framework on Digital Data Governance (2018), and ASEAN Model Contractual Clause for Cross Border Data Flow (MCCs 2021) and other international rules and mechanism to enhance digital trade that matches Cambodian context.

At the time of writing this article, the National Policy of Data Governance and Open Data and Cloud First Policy are still in drafting stage. Therefore, the data residence and/or data localization,

classification of data, international data transfer is in discussion among policymakers. Therefore, detail provisions on Data Storage and International data Transfer are to be determined in a separate regulations or Common Guidelines for Personal Data Protection.

Inspection, Dispute Resolution and Penalties

As part of the Cambodian legislation structure, personal data Inspection, personal data Dispute Resolution and Penalties are outlined in the PDPL.

The Minister of Ministry of Post and Telecommunications appoint personal data Inspection Officers to monitor, investigate, gather evidence, and strengthen the enforcement of PDPL. Personal data Inspection Officers receive legal status as judicial police to monitor offenses as stated in the PDPL and act in accordance with provisions of the Criminal Procedure Code. The PDPL establishes administrative complaint procedures against the Personal Data Inspection Officers. Any person who does not agree with any action taken by a Personal Data Inspection Officer may file a complaint to Ministry of Post and Telecommunications within 30 (thirty) days from the date of receipt of the decision. The Minister of Ministry of Post and Telecommunications is mandated to issue a decision on the complaint within 45 (forty-five) days from the date of receipt of the complaint. If such a person does not agree with the decision of the Minister of Ministry of Post and Telecommunications, he or she may file a complaint to other mechanisms of the Royal Government or to the court according to procedures.

Besides criminal offenses, all disputes related to PDPL affairs, a disputing party is required to file a complaint to the Unit in charge of Personal Data Protection for a resolution in accordance with existing procedures. The PDPL requires the Unit in charge of Personal Data Protection to conduct a conciliation or resolution of a dispute related to within 15 (fifteen) days and the result of the conciliation is recorded in a conciliation report. If the conciliation fails, Unit in charge of Personal Data Protection is require to refer the dispute to the Minister of the Ministry of Post and Telecommunications in order to be resolved according to procedure.

The PDPL defines two types of penalties such as administrative penalties and criminal penalties. The former includes written warning, fine, restriction, suspension, or revocation of license and other administrative punishments, and the latter includes criminal penalties determined the law and other criminal provisions of other laws. Any data controllers and data processors violate provisions of the personal data protection law will be subjected to either administrative penalties or criminal penalties depending on nature of offense and number of repetition of offenses.

Conclusion and Recommendations

As explained above, the PDPL was developed based on laws and policies across the globe with the purpose to have a harmonious existing laws in Cambodia and regional harmonization to promote digital trade but reflecting the Cambodia's political economy and context.

The PDPL sets 2 (two) years of grace period of preparation for the implementation of the law. This period allows the government and all stakeholders to work together and develop an effective implementation plan and mechanisms for personal data protection. That means the law will come into force after two years from the date of promulgation. The PDPL is expected to be passed within the mandate of the government of the 7th Legislature of the National Assembly.

The proposed implementation plan for the adopted PDPL includes *i) formulating implementation regulations, ii) developing Common Guidelines for Personal Data Protection , iii) Upskill data protection officers (DPO) through education and awareness raising programs for government, private sector and citizens to build culture of privacy and personal data protection, iv) establishing a public private partnership between the government, private sector, academia, civil societies and international organizations to share resources, information and best practice of tackling challenges on protection of privacy and personal data, v) etc..*

Personal Data Protection

Cross-Border Data Flow Mechanism: An Appropriate Approach for Cambodia

Sous Monirida

Abstract

The rapid growth of digital technologies and the worldwide interrelation of economies have amplified the importance of cross-border data flow. The cross-border data flow, enabling the seamless movement of information across boundaries, has emerged as a driver of innovation, economic growth, digital trade, and international cooperation. However, some concerns in relation to privacy, security, and regulatory compliance of data transfer have also been raised. These challenges require the development of robust mechanisms and frameworks to ensure the secure and lawful transfer of data across the border. To name a few, the standard contractual clause, certification, adequacy decision, and binding corporate rules. In particular, the increasing tendency for data localisation, requiring data to be stored in its sovereignty, heavily hinders the free flow of data. Hence, the appropriate policy to balance promoting data flow for economic benefits while safeguarding individual data rights is required. Considering the ongoing drafting of the Cambodia Law on Personal Data Protection, this paper will contribute to scholarly discourse on cross-border data flow, explore the mechanisms facilitating data transfer, and formulate an appropriate policy framework to govern cross-border data flow in Cambodia.

Introduction

With the increasing reliance on the internet in daily transactions, personal data become more readily accessible and consequently susceptible to potential risks. The ease of sharing personal information with unknown third parties is getting normalized in people's behavior that they often overlook the consequences of exposing personal information. Given the nature of globalization, data is being transferred every day around us ranging from when you swipe your credit card or purchase your plan ticket. Cross-border data transfer plays a crucial role in the globalization data economy. Multinational companies often transfer customers' data between various offices to offer diverse services or send the collected data abroad for processing or storing. Due to limited control and enforcement abroad, governments adopt various regulations and measures to regulate cross-border data transfers, aiming to protect individual's privacy and safeguard data deemed critical for nation.

General Data Protection Regulation (GDPR), which was introduced within the European Union (EU), has had a profound influence on data protection practices worldwide, leading many countries to subsequently adopt similar principles and definition from GDPR in their own data protection regulations. The three distinct paradigms in data regulation are subsequently recognized which are the conditional model, open model, and control model.[1] The "conditional model" prioritizes individual privacy rights while ensuring relatively free data flows for businesses which is seen in the GDPR.[2] On the other hand, the "open model" places greater emphasis on economic and business needs, resulting in minimal data transfer restrictions which are seen in countries like the U.S., Australia, and Singapore. Lastly, the "control model" emphasizes national security and public interests, leading to significant barriers in cross-border data flows to safeguard these interests which are implemented by China, Russia, and Vietnam.[3]

The data localization has also been arguably a tool to restrict the free flow of data which is implemented in a number of countries such as Indonesia, Nigeria, China, South Korea, Russia, India, Vietnam.[4] For instance, South Korea prohibits the transfer of mapping data outside of

1 Xie, Taojun, Jingting Liu, Ulrike Sengstschmid, and Yixuan Ge. 2023. "Navigating Cross-Border Data Transfer Policies: The Case of China." Asia Competitiveness Institute Research Paper Series, no.1 (April 2023).

2 Ibid.

3 Ibid.

4 Chander, Anupam, and Uyên P. Lê, "Data Nationalism." Emory Law Journal 64, no.3 (2015): 677.

their jurisdiction to protect national security.[5] Nigeria requires to host government data locally.[6] China and Russia require to store personal data inside the country.[7] Based on the research by Anupam Chander and Uyen P. Le on Data Nationalism, different governments provide different justifications for data localisation including promoting individual security and privacy, securing domestic economic development, enhancing law enforcement, and maintaining state sovereignty.[8] There are two conflicting ideas on the state intervention of cross-border data flow. One perspective claims that the intervention of the government is essential to prevent the misuse and mishandling of data which prevents violation of privacy and safeguarding data.[9] On the other hand, the overly stringent government intervention in data flow has a negative impact on business operations which could hamper international trade and adversely affect the country's business competitiveness.[10]

In Cambodia, the Ministry of Post and Telecommunications is presently in the process of drafting the Law on Personal Data Protection. While a comprehensive framework for personal data protection is yet to be established, the concept of data protection has been rooted in the constitution, civil code, and other sectoral regulations such as finance, telecommunications, legal, insurance, and healthcare.[11]

The forthcoming Law on Personal Data Protection is poised to encompass the principles and rules of collection, use, and disclosure of personal data, the rights of data subjects, the obligation of data controller, and the transfer of personal data. This paper, therefore, seeks to make an insightful contribution to a section of the draft Law concerning cross-border data transfer by enumerating the cross-border data transfer mechanisms that enables policymakers to make an informed decision on the approach they should adopt in Cambodia to strive for the balance of promoting data flow for economic benefits while safeguarding individual data rights.

Cross-border Data Transfer Mechanisms in EU, Singapore, and China

In this chapter, the paper will discuss the mechanisms adopted by EU, Singapore and China to safeguard the data flow across the border. The diverse regulatory approaches, with the EU setting comprehensive standards through GDPR, Singapore adopting pragmatic regulation, and China's strict data transfer requirements, will provide an insightful comparison to shape the data transfer landscape in Cambodia.

Cross-border Data Transfer Mechanisms in EU

In the EU, the Data Protection Directive (Directive 95/46/EC) of 1995 was the first framework to safeguard personal data across the EU while mandating each member state to adopt their own national data protection laws based on the directive.[12] In 2016, the General Data Protection Regulation (GDPR) was adopted and replaced the Data Protection Directive which aims to harmonize data protection law across the EU by providing a more consistent and robust framework

5 Ibid., 703.
6 Ibid., 700.
7 Ibid., 701-702.
8 Chander, Anupam, and Uyên P. Lê, Supra n 4, 713-739.
9 Unver, Hamid Akin. 2016. "Cross-Border Data Transfers and Data Localisation." EDAM Cyber Policy Paper Series 2016/3, June 2016.
10 Ibid.
11 Phin Sovath, "Privacy and Data Protection in the Digital Age: A Holistic Approach to Privacy and Data Protection in Cambodia," in Law in the Digital Age: Protection of Consumer Rights, ed. Kong Phallack and Long Chanbormey (Konrad-Adenauer-Stiftung, Cambodia, 2021):51-70.
12 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the European Parliament and of the Council, 24 October 1995.

for protecting personal data.[13] In terms of data transfer, the data can be transferred outside of the EU unless the GDPR's level of data protection is ensured through adequacy mechanism, safeguard mechanism, or derogation mechanism.

Transfer on the basis of an adequacy decision

The transfer of personal data to a third country is allowed if the European Union has determined that the third country provides an adequate level of data protection. In such cases, there is no need for any additional authorization for the data transfer.[14] The Commission assesses data protection adequacy in third countries based on factors such as (1) rule of law, respect for human rights and fundamental freedom, and relevant legislations in relation to personal data protection as well as the implementation of such legislation; (2) the existence and effectiveness functioning of independent supervisory authorities responsible for enforcing compliance with data protection rules; (3) international commitments and obligations related to the protection of personal data.[15] Upon the assessment, the adequacy decision is made through implementing act and such decision is subject to review which occurs at least every four years by taking into account the development of that particular third country.[16] In the event that the third country no longer satisfies an adequate level of protection, the Commission may repeal, amend or suspend the decision and enter into consultation with that third country to remedy the situation.[17] The Commission publishes the list of third countries which are deemed to provide an adequate level of protection or no longer.[18] Thus far, the European Commission has recognized following 14 countries as having adequate data protection includes Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay.[19]

Recently, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework which enables data controllers in the EU to transfer personal data to participating data recipient in U.S. without being subject to any further authorization.[20] This adequacy decision is a long waiting decision for the EU and U.S. companies after its precedent has been rejected by the Court of Justice of EU due to safeguard issue concerning data access by U.S. public authorities.[21]

Transfer subject to appropriate safeguard

In the absence of the adequacy decision, the data can be transferred to third country unless the controller or processor of the recipient country has provided an appropriate safeguard and there is enforceable data subject rights and effective legal remedies available to the dividual whose data is being transferred. Those appropriate safeguards which are required authorization from authorities include:

- ***Legal binding and enforceable instrument between public authorities or bodies:*** this mechanism applies to public authorities or body transferring to another public authorities

13 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, the European Parliament and of the Council, 27 April 2016 (Known as General Data Protection Regulation (GDPR)),

14 GDPR, Article 45.

15 Ibid., Article 45(2).

16 Ibid., Article 45(3).

17 Ibid., Article 45(5) (6).

18 Ibid., Article 45(8).

19 European Commission. "Adequacy Decision." accessed August 21, 2023. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. You can also find the Adequacy Decisions of the EU Commission for the 14 countries in this link provided.

20 European Commission. "Questions & answers: EU-US Data Privacy Framework." Accessed August 21, 2023. https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

21 Ibid.

or bodies in the third countries having signed the instrument that is legally binding and enforceable such as international treaties, public-law agreements, or self-executing administrative accords.[22]

- ***Binding corporate rules:*** A company subject to GDPR may use binding corporate rules as a safeguard to transfer personal data outside of the EU within a group of undertakings.[23] The binding corporate rules must be a legally binding instrument encompassing fundamental data protection principles and rights and upheld by every affiliates of the group.[24] The binding corporate rules are approved by the competent supervisory authority if they meet the criteria of (1) legally binding and applicable to all members of the group of undertakings engaging in joint economy activities, including employees, (2) grant enforceable rights to data subjects regarding their personal data processing, and (3) contain items as required by Article 47(2) of GDPR.[25]
- ***Standard contractual clauses:*** standard contractual clauses (SCCs) are pre-established and authorized sets of data protection clauses that enable data controller to safeguard an adequate level of protection of the transferred data outside of the European Economic Area (EEA).[26] The parties may incorporate the SCCs into the contract between parties or add additional clauses to the SCCs so long as the clauses do not contradict the SCCs or harm the data subject's rights.[27] Some jurisdictions have endorsed the EU's SCCs with minor adaptations to their domestic regulation while other jurisdictions developed their own model clauses that share several similarities with these SCCs.[28]
- ***Code of conduct:*** The data recipient uses and adheres to the code of conduct for the purpose of providing the appropriate safeguard to data transferred outside of the EU.[29] In other words, controller subject to GDPR can rely on the adherence to code of conduct by data recipients as having met their obligation under GDPR when transferring data to third countries without the need to adhere to the code themselves.[30] The code of conduct may be prepared by associations and other bodies representing controllers that are from the same sector or share the same processing characteristics and needs.[31] The code of conduct should contain essential principles as well as rights and obligations under GDPR and be submitted to the supervisory authority for approval and recognition by Commission.[32]
- ***Certification:*** Certification is a tool that demonstrates the existence of appropriate safeguards provided by the data importer on which the data exporter can rely to transfer the data outside of the EU.[33] Certification is issued by a certification body accredited by

22 European Data Protection Board, "Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data Between EEA and Non-EEA Public Authorities and Bodies" (18 January 2020).

23 European Commission. "Binding Corporate Rules (BCR)," Accessed August 21, 2023. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

24 Ibid.

25 GDPR, Article 47(1). The list of approved binding corporate rule in the EU as provided in this link: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en

26 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance). (2021). Official Journal of the EU, L 199, 31-61.

27 Ibid.

28 European Commission. "The New Standard Contractual Clauses – Questions and Answer.," accessed August 21, 2023. https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf.

29 European Data Protection Board. 2022. "Guideline 04/2021 on Codes of Conduct as tools for transfers, version 2.0." 6.

30 Ibid.

31 GDPR, Article 40(2); European Data Protection Board. 2022. "Guideline 04/2021 on Codes of Conduct as tools for transfers. version 2.0." 6.

32 GDPR, Article 40(5).

33 European Data Protection Board. 2023. "Guidelines 07/2022 on Certification as a Tool for Transfers, Version 2.0," 9.

supervisory authority based on the approved criteria while the data controller or data processor provides authority for all information and access to its processing activities which are necessary to conduct the certification procedure.[34] Certification is issued to the controller for a maximum of three years and can be renewed if they continue to meet relevant requirements.[35] However, if the requirements for certification are no longer met, the certification may be withdrawn by certification bodies.[36]

Derogation for specific situations

a. In the absence of either an adequacy decision or an appropriate safeguard, transferring personal data to third country is allowed under following conditions:[37]
b. Explicit consent from the data subject after being informed of the possible risks of such transfer. An example could be when a European consumer consents to their personal data being transferred to hotel located in non-EU country for vocation purpose.
c. Transfer necessary for contract performance between data subject and data controller or pre-contractual measures implementation at the data subject's request. An example could be when an EU resident buys a product from a Thai online retailer and the transfer of her address is necessary for the delivery of the product.
d. Transfer necessary for the conclusion or performance of a contract concluded in the data subject's interest between the controller and another natural or legal person. An example could be when an EU citizen has purchased medical insurance with an EU insurance provider and their medical data is transferred to an overseas hospital for treatment.
e. Transfer necessary for important public interests. An example could be the sharing of data between EU country and the U.S. on vaccines to address Covid-19 pandemic.
f. Transfer necessary for the establishment, exercise, or defense of legal claims. An example could be EU law firm transferring client's data to non-EU lawyer for a claim in a property case.
g. Transfer necessary to protect vital interests of the data subject or other person when the data subject is physically or legally incapable of giving consent. An example could be the transfer of medical data of EU citizens to overseas doctors in an emergency where that individual cannot provide consent due to their condition.
h. Transfer is intended to provide information to the public and open to consultation under Union or Member State law and meeting specific conditions. An example could be the sharing of information with international organizations for transparency purposes.

In cases where a transfer cannot rely on an adequacy decision or appropriate safeguard, nor any specific derogations apply, a transfer to a third country is permissible if the transfer is not repetitive, involves only a limited number of data subjects, is necessary to serve compelling legitimate interests pursued by the controller, provided that these interests do not override the rights and freedoms of the data subjects. In addition, the controller must thoroughly assess the circumstances of the data transfer and establish appropriate safeguards to protect the data. The controller must inform the transfer to the supervisory authority and then data subject about the transfer and compelling legitimate pursued.[38]

An example could be the EU-based financial institution needs to transfer a limited amount of customer data to an overseas partner bank to investigate a case of potential financial fraud. The transfer is necessary to serve a compelling legitimate interest in preventing financial crime and the data subject's rights and freedoms are not compromised.

34 GDPR, Article 42(5).
35 GDPR, Article 42(7).
36 Ibid., Article 42(7).
37 Ibid., Article 49(1).
38 GDPR, Article 49(1)

Cross-border Data Transfer Mechanisms in Singapore

Singapore adopted the Personal Data Protection Act (PDPA) in 2012 which was amended in 2020.[39] The act governs the collection, use, and disclosure of personal data in a manner that strives the balance between individual rights and the handling of data by the company for reasonable and appropriate purposes.[40] The controller must adhere to the Transfer Limitation Obligation in order to transfer data to other countries, meaning the controller cannot transfer the data outside of Singapore unless the transferred data is accorded a standard of protection that is comparable to that under PDPA.[41] To ensure comparable data protection standards as under the PDPA, the controller must ensure that recipients of the transferred data are bound by legally enforceable obligations. These obligations can be imposed through:[42]

- Law of the data recipient's country.
- Contracts specifying the required standard of data protection and the countries to which the data is transferred. The contract includes but not limited to the purpose of collection, use, and disclosure by recipient, accuracy, protection, retention limitation, policies on personal data protection, access, correction, and data breach notification.
- Binding Corporate Rules (BCRs) requiring recipients of transferred data to adhere to a similar standard of protection as the PDPA. The rules must address recipients, countries, and rights and obligations. The recipient which can utilize the BCRs must be related to the transferring company, in the form of direct or indirect control over each other, or they are both directly or indirectly controlled by a common entity.
- Any other legally binding instruments.

An alternative way to ensure legally enforceable obligation is when an overseas recipient company holds a "specified certification" granted or recognized under the law of the receiving country.[43] "Specified certification" refers to under the PDPA include certifications under the APEC Cross-Border Privacy Rules (CBPR) System and the APEC Privacy Recognition for Processors (PRP) System.[44] CBPR system is a certification program supported by APEC members that companies undergo the assessment to demonstrate their adherence to globally-recognized data protection standards under APEC Privacy Framework.[45] Once certified, the companies can transfer personal data across the border between APEC members.[46] While the CBPR applies to data controller, the PRP system is designed as a complementary that focuses on data processors.[47]

Singapore also recognizes and encourages to use of the ASEAN Model Contractual Clauses (MCCs) which are designed by ASEAN to provide appropriate safeguards for the transfer of personal data across the border.[48] The MCCs outline the fundamental responsibilities for collection, use, and disclosure, personal data protection measures, and data breach notification. The adoption

39 Personal Data Protection Act 2012, No. 26 of 2012 (20th November 2012); Personal Data Protection (Amendment) Act 2020, No. 40 of 2020 (25th November 2020).

40 PDPA 2012, 2020 Rev. ed., Article 3.

41 Ibid., Article 26.

42 Personal Data Protection Commission. "Advisory Guidelines on Key Concepts in the Personal Data Protection Act." issued 23 September 2013, revised 16 May 2022, 123.

43 Personal Data Protection Commission. Supra n 42.

44 Ibid.

45 Personal Data Protection Commission Singapore. "APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems." Accessed August 21, 2023 https://www.pdpc.gov.sg/help-and-resources/2021/10/apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems

46 Ibid.

47 Ibid.

48 Personal Data Protection Commission. "Advisory Guidelines on Key Concepts in the Personal Data Protection Act." issued 23 September 2013, revised 16 May 2022, 123.

of ASEAN MCCs is voluntary.[49] The controller may adapt the ASEAN MCCs to suit their business arrangement so long as it complies with PDPA as guided by the "Guidance for use of ASEAN Model Contractual Clauses in Singapore." [50]

In the event that the data controllers cannot rely on legally enforceable obligations, they can count on certain circumstances as follows: [51]

- Where consent is obtained by the data subject. An example could be a Singapore resident agrees to their email address being shared with an overseas marketing company for promotional offers.
- Where deemed consent is obtained from the data subject when the transfer is necessary for conclusion or performance of contract between data controller and data subject. An example could be a Singaporean customers provide passport's data to the Qatar airline to book a flight to Qatar.
- Where transfer necessary for use or disclosure that is in the vital interests of individual or in the national interest. An example could be Singapore share health data with WHO to address global pandemic.
- Where data is in transit, meaning personal data being transported through Singapore to another country without being accessed, used, or disclosed by any company except the transferring organization or its employees involved in the transportation process, and solely for the purpose of that transportation. An example could be shipping package from the U.S. to Cambodia contains the recipient's address as it travels through Singapore.
- Where data is publicly available in Singapore. An example could be a company that uses publicly accessible data from websites for academic research.

Cross-border Data Transfer Mechanisms in China

China has adopted three laws to regulate the data which include Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL). While The CSL requires Critical Information Infrastructure Operators (CIIOs) to store the data in China, the DSL requires localisation of "Important/Critical Data" generated by entities other than CIIOs.[52] The "Critical/ Important data" refers to "any data which if tampered with, damaged, leaked, or illegally acquired or used, may endanger national security, the operation of the economy, social stability public health and security. etc."[53] The PIPL extends further on the requirement of data localisation by seeking CIIOs and entities that process the personal data[54] collected and generated in China exceeding the threshold provided by the Cyberspace Administration of China (CAC) to store such data in China.[55] Such threshold includes: [56]

- Personal data or "important data" transferred are collected by CIIOs.

49 Ibid.

50 Personal Data Protection Commission. 2021. "Guidance for Use of ASEAN Model Contractual Clauses in Singapore." 2.

51 Personal Data Protection Commission. Supra n 48. 124.

52 Xie, Taojun, Jingting Liu, Ulrike Sengstschmid, and Yixuan Ge. Supra n 1.6.

53 Security Assessment Measure on Cross-Border Transfers of Data, Article 19; Office of the Privacy Commissioner for Personal Data, Hong Kong, "Mainland's Personal Information Protection Law," Accessed August 21, 2023, https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html#96.

54 For the purpose of consistency throughout this paper, personal data refers to personal information stated in Personal Information Protection Law (PIPL).

55 PIPL, Article 40, Accessed August 21, 2023, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

56 The Security Assessment Measures on Cross-border Transfer of Data, 7 July 2022, Article 4; Office of the Privacy Commissioner for Personal Data. Hong Kong. "Mainland's Personal Information Protection Law." Accessed August 21, 2023, https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html#96.

- Data transferred overseas includes "important data."
- Processor processing personal data of more than 1 million persons.
- Personal data of more than 100,000 persons or sensitive personal data[57] of more than 10,000 persons are transferred outside of China since 1 January of the previous year.
- Other circumstances as required by CAC.

Regarding cross-border data transfer, entities who wishes to transfer personal data to a recipient outside of China due to business purposes must satisfy one of the following conditions:[58]

- Pass the security assessment conducted by the CAC for the entities meet the threshold stated above. The data controller[59] must submit the security assessment report to CAC through local cyberspace administration authorities at the provincial level.[60] The approval of the security assessment of cross-border data transfer is valid for two years.[61]
- Obtain a personal data protection certification issued by a specialized agency recognized by CAC. The certification process consists of technical verification, on-site review, and post-certification supervision.[62] This certification is valid for three years and renewable where the approval of post-certification supervision is passed, and the requirements of the certification are met.[63]
- Enter into a contract stating both parties' rights and obligations with the foreign recipient in accordance with the template designed by CAC. The standard contract covers including but not limited to the responsibilities of the data controllers and the foreign recipient, the impact of the foreign recipient's regulation on the performance of the contract, individual's rights and remedies, and liability for contract breach.[64]
- Meet other requirements prescribed by laws, regulations, or by CAC.

If any international treaty or agreement that China has concluded or acceded contains specific requirements for transferring personal information outside of China, those requirements must also be adhered.[65]

Furthermore, a data controller is required to conduct a personal data protection impact assessment and keep a record of this assessment prior to transferring personal data outside of China.[66] Additionally, when a data controller transfers the data to a recipient outside of China, the data controller must obtain the data subject's separate consent and inform them about the names and contact information of the overseas recipients, the purposes and methods of processing, the types of personal data involved, and the procedures for exercising their rights under the PIPL.[67] Data controller must take necessary measures to ensure that overseas recipients process personal data in compliance with the personal data protection standards outlined in the PIPL.[68]

57 Sensitive personal data refers to personal information that, if leaked or used illegally, may lead to violation of dignity of natural persons, or may seriously endanger their personal or property safety. Sensitive data include data related biometrics, religious, specific identities, healthcare, financial accounts, an individuals address as well as personal information of minors under the age of 14.

58 PIPL, Article 38, Accessed August 21 2023, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

59 For the purpose of consistency throughout this paper, Data controller refers to personal data processor stated in Personal Information Protection Law (PIPL).

60 The Security Assessment Measures on Cross-border Transfer of Data, 7 July 2022; Office of the Privacy Commissioner for Personal Data. Hong Kong. "Mainland's Personal Information Protection Law." Accessed August 21, 2023, https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html#96.

61 Ibid.

62 Ibid.

63 Ibid.

64 Ibid.

65 PIPL, Article 38, accessed 21 August 2023, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

66 PIPL, Article 39.

67 Ibid., Article 39.

68 Ibid., Article 38.

Recently, CAC has released the draft regulation proposing exemption for data transfer mechanism under following conditions:[69]

- Transfer of non-personal or non-important data.
- Transfer of personal data that is not collected in China, however, being transit in China.
- Transfer of no more than 10,000 individuals' personal data per year.
- Transfer is necessary for the performance of the contract.
- Transfer is necessary for human resources management in compliance with labor laws.
- Transfer is necessary to safeguard the life, health, and property safety of individuals during emergencies.

The Comparison and Recommendations on Cross-border Data Transfer

Approach to Cross-border Data Transfer

Through a comparison of approaches each country takes in relation to cross-border data transfer, the three jurisdictions have enacted the legal frameworks, establish the relevant data protection authority, adopted various mechanisms to facilitate the cross-border data flow. The EU stands out for its robust commitment to data protection enshrined in the GDPR that laid out rigid comprehensive mechanisms and certain exceptions for transferred data. The EU's approach prioritizes individual privacy rights and data security, making them suitable for countries with a strong emphasis on data protection. Singapore has adopted a flexible approach that emphasizes organizational accountability, promoting business growth and innovation. In contrast, China has taken a distinct path by implementing data localization and a strict data transfer approach. China also requires data controller to store a copy of data within Chinese territory although the data are allowed to process overseas.

This paper recommends Cambodia take the approach that facilitates cross-border flow which allows transferring personal data outside of jurisdiction so long as the transferred data is accorded the adequate standard of protection as required under the Cambodia Personal Data Protection Law. The requirement to store personal data in Cambodia might do more harm than good considering the security, business competitiveness, and international best practices. Data localisation increases company operation costs, undermines innovation, and limit consumer choices. It is worth noting that the governmental data are required to be stored in Cambodia.[70] However, that does not mean personal data should be subject to localization as well. The country may classify certain data as critical and require local storage for national security purposes, but personal data should be allowed to flow freely enable people to exchange information, provide cross-border services, and leverage the technology.

Cross-border Data Transfer Mechanisms

The three jurisdictions allow data transfers across the border as long as the recipient can ensure standard of protection to the transferred data comparable to the protection under their laws. The recipient can demonstrate the "standard of protection" through various mechanisms, with the EU through adequacy decisions, safeguard mechanisms, and derogation circumstances while Singapore enforces through legally enforceable obligations. China, however, imposes further strict requirements for certain entities falling into the defined threshold to undergo a rigid security

69 Herbert Smit Freehills. "China relaxes measures on cross-border data transfers from China." Accessed October 21, 2023, https://hsfnotes.com/data/2023/10/03/china-relaxes-measures-on-cross-border-data-transfers-from-china/#:~:text=Exemptions%20from%20cross%2Dborder%20data%20transfer%20mechanisms&text=Personal%20information%20which%20is%20not,the%20cross%2Dborder%20transfer%20mechanisms. Cooley. "China Loosens Cross-Border Data Transfers Controls." Accessed October 21, 2023. https://cdp.cooley.com/china-loosens-cross-border-data-transfer-controls/

70 Sub-Decree on Management, and Use of National Domain Names on the Internet, 31 December 2021, Article 6.

assessment when transferring data overseas in addition to data localization requirements.
EU is the only one among the three countries that would assess the "equivalent level of protection" based on adequacy criteria. The adequacy decision eases compliance for EU-based companies by permitting automatic data transfer to countries with an approved level of protection while putting the burden on the European Commission to regularly conduct the assessment. Nevertheless, China's security assessment could potentially impede the data flow across borders. Such restrictions may hinder international business operations and data-driven activities, potentially affecting economic growth and innovation. These two approaches may not be well suited to Cambodia's long-term interests, legal complexity, and the maturity of Cambodia's data protection standard.

Aside from adequacy decisions and security assessment, the three jurisdictions have shared common safeguard mechanisms including certifications, contracts, binding corporate rules, and legally binding instruments.

Standard Contractual Clauses

All three jurisdictions acknowledge the use of standard contractual clauses as a tool for facilitating cross-border data transfers. Data controller seeking to transfer data beyond their respective jurisdictions can engage in agreements known as standard contractual clauses with foreign recipient companies. Each jurisdiction's competent authorities have created their own models of these contractual clauses, which data controller may incorporate into their contracts. For instance, the EU's Standard Contractual Clauses (SCCs) offer a comprehensive set of clauses that encompass various transfer scenarios, allowing companies to choose the specific module that suits their situation, be it controller to controller, controller to processor, processor to processor, or processor to controller. Furthermore, within the ASEAN member states, the ASEAN Model Contractual Clauses (MCCs) are available as a baseline set of contractual clauses that data controllers can adapt to their business needs when conducting cross-border data transfers.
Certification

EU, Singapore, and China share the recognition of certification as a tool to demonstrate the existence of an equivalent level of protection accorded by the data recipients. In the EU, the data recipient is required to obtain a certification issued by accredited third-party certification bodies to indicate that its processing of personal data complies with requirements under GDPR. Singapore does not design their own certification, however, recognizes certifications under the APEC Cross-Border Privacy Rules (CBPR) System and the APEC Privacy Recognition for Processors (PRP) System obtained by data recipients.

Binding corporate rules

Legally binding corporate rules (BCRs) are recognized mechanisms in the EU and Singapore for governing cross-border data transfers within multinational group companies. Affiliates within these groups that handle data must adhere to the BCRs containing measures to protect the data being transferred. These BCRs must then be submitted for approval to the relevant competent authority. Upon approval, affiliates are granted the flexibility to customize the template to suit their specific needs, eliminating the need for individual contracts for each data transfer. In comparison to certifications, BCRs offer companies significantly more flexibility and the advantage of consolidating all data processing activities within a single comprehensive document.

Code of Conduct and other mechanisms

The EU adopted the Code of Conduct as one of the cross-border data transfer tools, while China and Singapore do not explicitly address this mechanism in their regulations. Code of conduct can

be utilized by the association from the same sector, or share the same processing characteristics and needs despite coming from different sectors.

Legally binding instruments

All three jurisdictions permit data to be transferred to overseas recipients based on the use of legally binding instruments. In the EU, these binding instruments must be established between public authorities while Singapore makes reference to the laws of the recipient country. Likewise, China allows such transfers as required under international treaties they have entered into.
The paper recommends that Cambodia should consider adopting the aforementioned mechanisms as essential tools to ensure standardized protection of data transferred across its borders. Besides legally binding instruments, Contractual clauses, certifications, binding corporate rules, and codes of conduct offer flexibility for data controllers to choose and tailor to their specific needs. By embracing these mechanisms, Cambodia can build trust with stakeholders, simplify compliance for companies, reduce costs, and harmonize with global data protection standards. To facilitate this adoption, Cambodia should consider leveraging existing regional and international models of these mechanisms, alongside developing its own models as needed and establishing a specialized agency to continuously monitor data recipients' compliance to maintain data protection standards.

The derogation under certain circumstances

Besides the safeguard mechanisms mentioned above, the EU, Singapore, and China also permit cross-border data transfers under specific exceptions. These exceptions balance data protection with specific scenarios where data transfer is justified. The common exceptions include scenarios where data transfers are allowed:

- When the data subject has provided explicit consent for the transfer.
- When the transfer is necessary for the performance of a contract.
- When the transfer is essential to protect someone's vital interests
- When personal data is data in transit
- when personal data is publicly accessible

While the terminology used may vary between these regions, the underlying concepts are quite similar. For example, Singapore allows transfers for "national interest," which is akin to the EU's allowance for transfers necessary for "public interest." Similarly, China permits the transfer of fewer than 10,000 individuals' personal data within a year, a concept similar to the EU's provision that allows transfers that are not repetitive and involve a limited number of data subjects for the purpose of compelling legitimate interests. Despite this, each jurisdiction also has its own specific exceptions. For instance, the EU allows data transfer for legal claims and China allows data transfer necessary for human resources management purposes.

This paper recommends Cambodia consider adopting derogations within its data protection framework to enable specific circumstances where cross-border data transfers are permissible. To do so effectively, Cambodia should align these exceptions with international data protection standards, and clearly define and limit the circumstances under which transfers are allowed. Cambodia should consider adopting the exceptions which commonly shared by the EU, Singapore and China. This approach will strike a balance between enabling data transfers for legitimate reasons, such as consent, contract performance, vital interests, and public or national interest, while maintaining a high level of data protection.

Conclusion

In the contemporary digital landscape, the seamless flow of data across borders is essential for economic growth, data resilience, and technological development. A robust data protection regime should not only ensure the security of individuals' data but also actively promote and facilitate this free flow of data. To provide Cambodia with an insightful guide for shaping its approach to cross-border data transfer mechanisms, this paper has conducted a comparative analysis of the approaches and mechanisms employed by the EU, Singapore, and China.

Given Cambodia's ongoing digital transformation and the complex challenges associated with cross-border data transfer, it is imperative to strike a delicate balance between fostering economic development and safeguarding individuals' data. Therefore, this paper recommends that Cambodia allows cross-border data transfers, provided that the transferred data is treated with the same level of protection mandated by Cambodia's Personal Data Protection regulations. While requiring governmental data to be stored exclusively within Cambodia is a valid approach, it may not be a suitable strategy for personal data. In terms of transfer mechanisms, Cambodia can consider a range of mechanisms, including standard contractual clauses, certifications, binding corporate rules, codes of conduct, and legally binding instruments. Apart from these mechanisms, certain exceptions should be allowed to facilitate the data transfer across borders. These exceptions may include scenarios where data subjects provide consent, cases related to vital interests, data in transit, and situations involving the performance of contractual obligations. For the effective adoption of these data transfer mechanisms, Cambodia should establish a robust legal framework with clear guidelines for the handling and transfer of personal data. Customizing these mechanisms to accommodate the unique needs of different entities and ensuring their compatibility with data protection regulations in the respective jurisdictions where they will be applied are top priorities. Furthermore, Cambodia should evaluate its operational capacity to enforce and regulate data protection laws effectively, which includes the establishment of a competent authority responsible for data protection and the allocation of necessary resources to fulfill its functions.

These recommendations are designed to assist Cambodia in establishing a strong data protection framework that fosters trust, promotes international data flows, and safeguards individuals' data rights in an increasingly data-driven global environment.

Table of Comparison				
		EU's GDPR	**Singapore's PLPA**	**China's PIPL**
Cross-border data transfer Mechanisms	Adequacy decision	√		
	Security Assessment			√
	Standard Contract	√	√	√
	Certificate	√	√	√
	Binding Corporate Rules	√	√	
	Code of Conduct	√		
	Legally binding instrument	√	√	√
Derogation	Explicit consent from the data subject	√	√	
	Transfer necessary for contract performance between data subject and data controller	√	√	√
	Transfer necessary for the conclusion or performance of a contract concluded in the data subject's interest between the controller and another natural or legal person.	√		
	Transfer necessary for important public interests/national interest	√	√	

	Transfer necessary to protect vital interests of the data subject	√	√	√
	Transfer necessary for the establishment, exercise, or defense of legal claims	√		
	Transfer is intended to provide information to the public and open to consultation	√		
	Personal data is in transit		√	√
	Publicly available personal data		√	
	Transfer for Human resources management purposes			√
	Transfer less than 10,000 individual's personal data within one year			√
	Transfer is not repetitive and involves only a limited number of data subjects, is necessary to serve compelling legitimate interests pursued by the controller, provided that these interests do not override the rights and freedoms of the data subjects.	√		

Personal Data Protection

Data Protection Competition in the Digital Age: Proposed Regulatory Approach for Cambodia

Keo Sothie & Ros Sophearathna

Abstract

Data has been often described as the new oil, except data never runs out. The Royal Government of Cambodia has embarked on an ambitious digital transformation journey to create a data-driven economy and society. Many businesses in Cambodia rely on data for their operations. While the use of data can exponentially increase efficiency and provide additional benefits to businesses, it also increases concerns regarding privacy, data protection, and competition.

Generally, privacy and data protection have not been part of competition assessments. Competition regulators have never really considered privacy or data protection issues when assessing whether there is an abuse of dominance when a firm adopts a certain method or policy for processing data, or whether a merger harms the market. This article will examine legal trends and cases from the European Union and recommend policies for Cambodia to adopt to address privacy and data protection issues that may arise in competition.

Introduction: Data, Privacy, and Competition

The world is in the middle of a dynamic digital transformation. Buzzwords such as big data, cloud, smart city, internet of things, and especially artificial intelligence (AI) have become increasingly commonplace. Each day, 402.74 million terabytes of data are created.[1] Ninety percent of the world's data is estimated to have been generated in the last two years, and it is expected to increase exponentially in the coming years.[2] The popular chatbot from OpenAI, ChatGPT, reached 100 million monthly active users just two months after launch, setting the record for the fastest growing userbase.[3] This digital transformation period has been termed as the digital age or the Fourth Industrial Revolution.[4]

During this digital transformation period, data has been thought of as the new oil—an immensely valuable asset that has the vast potential to fundamentally change how organizations operate.[5] Data is collected about everything you do, including the movies you stream, the people you communicate with, the route you drive, and the amount of time you look at a picture on your phone .[6]

Data allows organizations to derive valuable insights for any business activity including understanding consumer behaviour, formulating new revenue models, creating advertisement campaigns, improving decision-making, forecasting and allowing for better consumer segmentation and targeting, and transforming work processes.[7] For governments, the insights from data allow

1 Fabio Duarte, "Amount of Data Created Daily," *Exploding Topics* (blog), April 3, 2023, https://explodingtopics.com/blog/data-generated-per-day.

2 Ibid.

3 Krystal Hu, "ChatGPT Sets Record for Fastest-growing User Base-analyst Note," *Reuters*, February 2, 2023, https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.

4 Klaus Schwab, "The Fourth Industrial Revolution: What It Means, How to Respond," *World Economic Forum*, January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

5 Joris Toonders, "Data is the New Oil of the Digital Economy," *WIRED*, accessed May 8, 2024, https://www.wired.com/insights/2014/07/data-new-oil-digital-economy.

6 "The World's Most Valuable Resources is No Longer Oil, But Data," *The Economist*, May 6, 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

7 Nisha Talagala, "Data as the New Oil is Not Enough: Four Principles for Avoiding Data Fires," *Forbes*, May 2, 2022, https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/; "Big Data: Bringing Competition Policy to the Digital Era," *OECD*, accessed July 28, 2024, https://web-archive.oecd.org/temp/2022-02-21/414870-big-data-bringing-competition-policy-to-the-digital-era.htm.

them to be more efficient by reducing time spent, duplicate work, and public spending, while providing faster and better public services, and being more effective at responding to the needs of the public.[8]

For these reasons, the largest and most powerful technology companies have structured their business models based on the collection and processing of voluminous data or "big data," and are engaged in fierce competition.[9] The importance of data is heightened with AI techniques that allow firms to process and extract value from such voluminous amounts of data—AI algorithms can forecast and make predictions about a consumer, such as when a consumer is ready to buy a product, an engine needs servicing, or a person is at increased risk of a disease.[10] This has resulted in technology companies racing to be the industry leader in the development and deployment of AI.[11] However, this voluminous data collection creates increased risks of violation of privacy and unfair competition.

Andreas Mundt, President of the Federal Cartel Office ("FCO"), Germany's national competition regulatory agency, states that powerful technology companies "knows you better than your wife."[12] Information is power, and the more data that is gathered by these technology companies, the more power they possess. The ability to collect vast amounts of data and process and extract value from them creates an addictive quality—a strong incentive for companies to collect and surveil with little regard for privacy.

The legal concept of privacy takes many different forms ranging from the right to freedom from intrusions by the state, especially in one's own home, to the right to control one's image and dignity.[13] Privacy also provides us with a "breathing room to engage in the processes of boundary management that enable and constitute self-development."[14] Privacy allows us to form an identity that is not dictated by social conditions—it provides a "breathing room" for innovation, for critical thinking, and for human flourishing.[15]

Mr. Mundt explains that because these companies are so dominant, consumers are forced to share their personal data if they want to search the internet or be on social media.[16] The dominance of technology companies is unique. Traditional antitrust laws and regulations only considers consumer welfare[17] and could never have imagined the access to data and networking that these firms possess. The collection of vast amounts of data can lead to monopoly positions[18] or "data-opolies" that could be harmful for competition and privacy.[19]

8 Cambodia Digital Government Policy 2022-2035, Royal Government of Cambodia, January 28, 2022, i.

9 "Big Data: Bringing Competition Policy to the Digital Era."

10 "The World's Most Valuable Resources."

11 Nico Grant and Karen Weise, "In A.I. Race, Microsoft and Google Choose Speed Over Caution," *The New York Times*, April 10, 2023, https://www.nytimes.com/2023/04/07/technology/ai-chatbots-google-microsoft.html.

12 Adam Satariano, "Big Tech 'knows You Better Than Your Wife.' He Plans to Rein it in," *The New York Times*, July 7, 2019, https://www.nytimes.com/2019/07/07/business/facebook-google-antitrust-germany.html.

13 James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *The Yale Law Journal* 113 (2004): 1151-1221.

14 Julie E. Cohen, "What Privacy is for," *Harvard Law Review* 126 (2013): 1904-1933.

15 Ibid., 1926-1927.

16 Satariano.

17 Giuseppe Colangelo and Mariateresa Maggiolino. 2018. "Data Accumulation and the Privacy-Antitrust Interface: Insights from the Facebook Case for the EU and the U.S." *Stanford Law School and the University of Vienna School of Law TTLF Working Paper* 31 (2018): 25.

18 "Big Data: Bringing Competition Policy to the Digital Era."

19 Maurice E. Stucke. "Should We Be Concerned about Data-opolies." *Georgetown Law Technology Review* 2 (2018): 275-324.

Recognizing the importance of the right to privacy and data protection, the European Union has taken the lead in adopting a comprehensive data protection framework called the General Data Protection Regulation ("GDPR"),[20] which has become the gold standard for personal data protection. The GDPR has inspired many privacy and data protection laws and regulations in countries around the world. However, even with personal data protection rules, companies still use questionable methods for collecting and processing data to gain a competitive edge. In this digital age, it is imperative that antitrust rules adapt and can consider infringements on personal data protection and privacy rules when assessing competition.

Because of the intertwining between data and competition, this digital age requires a new approach to antitrust that considers privacy and data protection. Competition has changed in the digital economy though the rise of modern business strategies, mergers and acquisitions amongst dominant position companies, and the controversial market power achieved from such strategies.[21]

Cambodia's Digital Transformation Journey and Its Laws and Regulations Related to Data Protection and Competition

These risks to competition and privacy should be considered by the Kingdom of Cambodia, especially when the Royal Government's mandate is to prioritize digital transformation. The Royal Government recently adopted the Digital Economy and Society Policy Framework 2021-2035 in May 2021 with the vision of "building a vibrant digital economy and society by laying the foundations for promoting digital adoption and transformation in all sectors of society—the State, citizens, and businesses—to promote new economic growth and improve social welfare based on the new normal."[22] In January 2022, the Royal Government adopted the Digital Government Policy 2022-2035 with a vision of "establishing digital government to improve the citizens' quality of life and build their trust through better public service provision."[23] Furthermore, technology has been added as a key priority within the recently adopted Pentagonal Strategy, a long-term socio-economic strategy introduced by the Royal Government to the Seventh Legislature of the National Assembly. Pentagon 5 – Development of Digital Economy and Society includes building a digital government and digital citizens; development of digital economy, digital business, e-commerce, and digital innovation system; building and development of digital infrastructures; trustworthiness building in digital system; and development of financial technology.[24] In line with the Royal Government's policies and strategies, the Ministry of Post and Telecommunications ("MPTC") is drafting key laws and regulations to ensure that Cambodia's digital transformation is successful, which include a cybersecurity law and personal data protection law.

As for competition, Cambodia has some existing laws and regulations that regulates unfair competition. Starting with the Constitution, Article 56 states that Cambodia shall embrace the market economy system.[25] On October 5, 2021, Cambodia adopted the Law on Competition "as a framework for promoting competition, strengthening industrial structure, establishing

20 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119/1).

21 Filipe Da Silva and Georgina Núñez, "Free Competition in the Post-Pandemic Digital era: the Impact on SMEs," *Economic Commission for Latin America and the Caribbean*, 2021, https://repositorio.cepal.org/server/api/core/bitstreams/678a8494-f76e-4514-9963-a90622a1ff2e/content.

22 "Cambodia Digital Economy and Society Policy Framework 2021-2035," Royal Government of Cambodia, May 10, 2021, xi.

23 "Cambodia Digital Government Policy 2022-2035," ii.

24 "Pentagonal Strategy-Phase I for Growth, Employment, Equity, Efficiency and Sustainability: Building the Foundation Towards Realizing the Cambodia Vision 2050," Royal Government of Cambodia, August 24, 2023, 13.

25 Constitution of the Kingdom of Cambodia, September 21, 1993, art. 56.

mechanisms for law enforcement and promoting a competitive culture" in order to strengthen and develop the national economy.[26] The Law on Competition[27] and Sub-Decree on the Organization and Functioning of the Cambodia Competition Commission ("CCC") established the CCC with the purpose of effectively promoting the implementation of the Law on Competition and helping consumers to receive goods and services of high quality, low cost, and that are plentiful with various choices.[28] Just like other competition laws, Cambodia's Law on Competition prohibits activities that may distort competition in the Cambodian market. There are three main prohibitions: anti-competitive agreements which prevent, restrict or distort competition; abuses of dominant market positions; and anti-competitive business combinations.[29]

It is important to note, however, that competition regulation is not completely consolidated with the CCC. For example, the Law on Telecommunications provides competition regulatory powers within the telecommunications sector to MPTC and the Telecommunication Regulator of Cambodia ("TRC").[30] In line with this, the Sub-Decree on Conditions and Procedures of Business Mergers, established under the Law on Competition, acknowledges that the scope of the Sub-Decree shall not cover mergers within sectors that already have existing laws and regulations that govern such activities.[31]

MPTC's authority also extends to the information and communications technology ("ICT") sector. Article 26 of the Law on E-Commerce prescribes that an "intermediary and an electronic commerce service provider shall request for a permission letter or license from the Ministry of Commerce and the Ministry of Post and Telecommunications," with MPTC being the entity that issues the certificate for online service.[32] In addition, the Sub-Decree on the Authorization for Operation in the ICT Sector further prescribes MPTC with the power to regulate the ICT sector through the issuance of various ICT permits, certificates, and licenses.[33] Cambodia's competition regulatory framework is both centralized within the CCC, but also sectoral for heavily regulated sectors such as telecommunications.

Cambodia is embarking on an ambitious and dynamic digital transformation journey with an immense potential for economic growth. As Cambodia continues to develop into a digital economy and society, it has the advantage of learning lessons from developed data-driven countries. This paper will examine legal trends and cases from the European Union and propose considerations for Cambodia to adopt within its own legal framework and context in order to pre-empt and address privacy and data protection issues that may arise in competition. Section III analyses recent legal trends and major cases that involve privacy and data in competition assessments, specifically regarding abuse of dominant position and mergers. Section IV examines the applicability of these legal trends and cases within the Cambodian context. Lastly, Section V concludes and considers Cambodia's future on competition and privacy and data protection.

26 "Competition Commission of Cambodia," Ministry of Commerce, accessed September 24, 2023, https://www.ccfdg.gov.kh/en/commission-committee/new-title-2/.

27 Law on Competition, Royal Decree NS/RKM/1021/013, October 5, 2021, art. 4.

28 Sub-Decree No. 37 ANKR.BK on the Organization and Functioning of the Cambodia Competition Commission, February 17, 2022, art. 1.

29 Law on Competition, chap. 3.

30 Law on Telecommunications, Royal Decree NS/RKM/1215/01. December 17, 2015, chap. 10.

31 Sub-Decree No. 60 ANKR.BK on Conditions and Procedures of Business Mergers, March 6, 2023, art. 2.

32 Law on E-Commerce, Royal Decree NS/RKM/1119/017, November 2, 2019, art. 26.

33 Sub-Decree No. 110 ANKR.BK on the Authorization to Operate Information and Communications Technology, July 21, 2017.

European Union Legal Trends and Case Studies: Data Privacy and Competition

In 2021, Commissioner Lina M. Khan, of the Federal Trade Commission ("FTC") of the United States, issued a statement on privacy and security. In the statement, she discusses "the overlap between data privacy and competition" and "the growing recognition that persistent commercial data collection implicates competition as well as privacy":

> *[C]oncentrated control over data has enabled dominant firms to capture markets and erect entry barriers, while commercial surveillance has allowed firms to identify and thwart emerging competitive threats. Monopoly power, in turn, can enable firms to degrade privacy without ramifications—as the Commission itself recently alleged in court. Given that the competitive significance of data has been under-appreciated by enforcers across the board, breaking down siloes to better grasp these interconnections is key to ensuring rigorous analysis and effective enforcement.34*

In addition to the US, many other countries are conducting antitrust investigations into the most powerful technology companies for alleged infringements of competition rules and data privacy.[35] The EU is the leading jurisdiction in enforcing competition rules and incorporating data protection and privacy concerns into their competition assessments. This section will discuss how the EU has approached abuse of dominant position business practices through the European Court of Justice ("ECJ") *Meta* Case,[36] and mergers through the European Commission's approval of Microsoft's acquisition of LinkedIn ("*Microsoft/LinkedIn* Case").[37]

The European Court of Justice Meta Case—Abuse of Dominant Position

Technology companies have greatly benefited from network effects compared to brick-and-motor companies. Their multiple network effects contribute to a powerful feedback loop that attracts not only users, but also sellers, app developers, and advertisers:[38] through the collection of more data, a company has more capability to improve its product, which attracts more users, generating more data, continuing this feedback loop.[39] These network effects also create barriers to entry as it is difficult and costly to achieve the same economies of scale and attract users from other established networks.[40] In particular, small firms that rely on the use of data as an essential facility, face major challenges to their survival in the market due to the ability of the dominant companies to restrict access to data.[41] It is no coincidence that these entrenched technology companies remain unchallenged.

34 Lina M. Khan, "Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security Commission," *Office of the Chair, Federal Trade Commission*, October 1, 2021, https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf.

35 "Digitalization, Big Tech and Copycat Antitrust Investigations," *Norton Rose Fulbright*, March 2023, https://www.nortonrosefulbright.com/en/knowledge/ publications/74c278e8/digitalization-big-tech-and-copycat-antitrust-investigations.

36 Court of Justice of the European Union, *Meta Platforms Inc and Others v Bundeskartellamt*, Judgment of the court, Grand Chamber, July 4, 2023, C 252/21, ECLI:EU:C:2023:537.

37 Directorate-General for Competition, European Commission, *European Commission Decision of Microsoft/LinkedIn Case*, December 6, 2016, Case No. COMP/M.8124-Microsoft/LinkedIn.

38 Stucke, 282; see also Maurice E. Stucke, *In Breaking Away: How to Regain Control over Our Data, Privacy, and Autonomy*, (Oxford: University Press, 2022), 7.

39 "The World's Most Valuable Resources."

40 Stucke, *In Breaking Away*, 7.

41 Bruno Lasserre and Andreas Mundt, "Competition Law and Big Data: the Enforcers' View," *Italian Antitrust Review* 1 (2017): 91.

Data stifles competition as it allows technology companies to be gods of their own markets and beyond. They own app stores, social media platforms, operating systems, and even rent out computing power to startups. They can see rising products or services, which allow them to buy or copy them before they grow to even become a threat.[42]

The Court of Justice in the ground-breaking ECJ *Meta* case, held that a competition regulator may consider a dominant company's compliance with other rules than just competition when examining an abuse of a dominant position. On February 7, 2019, the FCO prohibited Meta from combining user data from different sources. The FCO imposed on Meta restrictions on its data collecting and processing practices. Under its terms and conditions, Meta could collect and combine user data on the Facebook website, Meta-owned services such as WhatsApp and Instagram, and third-party websites and apps, and then assign them to the user's Facebook account.[43] Because of Meta's dominant position, this created a false choice, forcing users to either use Meta services and share their data, or stay off not just Facebook but all of its social networks and its apps.[44] This FCO decision is the first time an EU competition authority has considered data protection rules as an important element in a competition assessment.[45]

Meta is a dominant company in the German market for social networks. In 2018, Meta had a market share of more than 95 per cent (23 million daily active users) and more than 80 per cent (32 million monthly active users).[46] Because of its dominant position, Meta has increased obligations under competition rules, especially since Meta users have little choice in switching social networks. Mr. Mundt explains:

> *[A]s a dominant company Facebook is subject to special obligations under competition law. In the operation of its business model the company must take into account that Facebook users practically cannot switch to other social networks. In view of Facebook's superior market power, an obligatory tick on the box to agree to the company's terms of use is not an adequate basis for such intensive data processing. The only choice the user has is either to accept the comprehensive combination of data or to refrain from using the social network. In such a difficult situation the user's choice cannot be referred to as voluntary consent.*[47]

Moreover, Meta was able to collect "an almost unlimited amount of any type of data from third party sources" and assign this data to users' Facebook account, creating a detailed profile of each user with knowledge of what they are doing online.[48] The FCO worked closely with leading data protection authorities and found that Meta's conduct was an abuse of its dominant position—its conduct represented an exploitative practice, impeding competitors that do not have access to such vast quantities of data.

42 "The World's Most Valuable Resources."

43 "Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources," Bundeskartellamt, February 7, 2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

44 Santariano, Adam, "Meta Loses Appeal on How It Harvests Data in Germany," *The New York Times*, July 4, 2023, https://www.nytimes.com/2023/07/04/business/meta-germany-data.html.

45 Deirdre Carroll et al., "EU's Top Court Rules that Competition Authorities Can Consider Data Protection Breaches in Their Investigation," *JD Supra*, July 7, 2023, https://www.jdsupra.com/legalnews/eu-s-top-court-rules-that-competition-5448636/.

46 "Bundeskartellamt Prohibits Facebook."

47 Ibid.

48 Ibid.

On February 11, 2019, Meta brought an action against FCO's decision before the Higher Regional Court of Düsseldorf. The Higher Regional Court had doubts as to the ability of national competition authorities in monitoring compliance with the GDPR and so it stayed the proceedings and referred to the ECJ clarifying questions.[49] The Court of Justice held that:

> *In the context of the examination of an abuse of a dominant position by an undertaking on a particular market, it may be necessary for the competition authority of the Member State concerned also to examine whether that undertaking's conduct complies with rules other than those relating to competition law, such as the rules on the protection of personal data laid down by the GDPR.50*

The Court of Justice found that the compliance or non-compliance of the conduct with the GDPR may provide a clue among other relevant circumstances to establish whether the conduct entails methods governing normal competition and to assess the conduct's consequences to the market or consumers.[51] While the finding of non-compliance with the GDPR does not necessarily mean there has been an abuse of dominant position *per se*, but such examination is relevant for competition assessments.

Importantly, the Court of Justice noted that a competition authority may examine whether a firm's conduct complies with the GDPR only in the context of the examination of an abuse of a dominant position, and that the competition authority must consult and cooperate sincerely with the data protection authority, while observing their respective powers and competences.[52] Furthermore, the competition authority must consult and seek the cooperation of the data protection authority to remove any doubt regarding GDPR compliance, or determine whether it must wait for a decision from the data protection authority before initiating its own assessment.[53]

Microsoft/LinkedIn Case—Mergers and Acquisition

The purpose of big data related merger and acquisition cases is usually to combine datasets that can allow for improved goods and services. Data concentration may allow for the merged entity to obtain a competitive advantage because it provides access to additional data. This also happens when the merger is between a firm from the upstream market and another firm from the downstream market. For example, online service providers may want to merge with software or hardware producers to gain access to data collected by the downstream companies. Consequently, the costs for competitors to extract the same data and provide the same quality will increase creating a competitive edge that could be harmful to the market and increase barriers for competitors.[54]

When the merged entity exclusively owns the data, it can even restrict access to the data in the upstream market that would have otherwise been supplied in the downstream market if such merger had not taken place. This would increase the costs for competitors in the downstream market since it would be more difficult for them to obtain data for the same prices and terms as before the merger. A merged entity could raise the costs on its consumers while restricting access to the data from its competitors.[55]

49 *Meta Platforms Inc and Others v Bundeskartellamt*, paras 31-34.
50 Ibid., para. 38.
51 Ibid., para. 47.
52 Ibid., para. 54.
53 Ibid., para. 57.
54 Oskar Törngren, "Mergers in Big Data-driven Markets-Is the Dimension of Privacy and Protection of Personal Data Something to Consider in the Merger Review," *Stockholm University* (2017): 31-32.
55 Ibid.

In general, the European Commission's approach to big data-related mergers has usually been to avoid over-enforcement.[56] The Commission may have adopted this approach because there is trust that efficiencies could result from such mergers; technology firms are supposedly always exposed to disruption by competitors; and although there is no evidence of efficiencies or innovation that would disrupt the market, there is a belief that the barrier in data-related markets is low because of data's ubiquity and the non-rivalry nature of information contained in data.[57]

In the *Microsoft/LinkedIn* Case, Microsoft sought to acquire LinkedIn through the purchase of all LinkedIn shares.[58] The Commission assessed whether there were any competition concerns resulting from the data concentration between Microsoft and LinkedIn post-merger.[59] The Commission noted that there are two main ways in which a merger may raise horizontal concerns when the two datasets previously held by two independent firms are concentrated under the ownership of the merged entity. First, the data concentration post-merger may increase the merged entity's market power over the supply of this data or increase barriers in the market for competitors who need the data to operate. Second, if the two independent firms were competing with each other on the basis of the data, then the merger would eliminate this competition.[60]

The Commission found that Microsoft and LinkedIn's merger did not raise these types of concerns in the context of online advertising because both entities, with limited exceptions, do not make their data available to third parties and the resulting data concentration did not raise barriers in the market as there continues to be a large amount of user data available for advertising purposes that are not within Microsoft's exclusive control. In addition, the Commission considered both Microsoft and LinkedIn to be small market players in online advertising and that they compete against each other limitedly.[61]

On privacy related concerns, the Commission found that such concerns are an important parameter of competition because it is a "driver of customer choice in the market for [professional social network] services."[62] Consumers have been increasingly valuing the privacy and security provided by a platform, and at times make their choices dependent on the level of privacy offered. For example, when Facebook announced that it was acquiring WhatsApp in 2014, thousands of users switched to other messaging platforms, particularly Telegram because it offered increased privacy protection.[63] When there are fewer options available, users are forced to use the platforms of a few technology companies and accept privacy policies that extensively collect and process data. As a result, the Commission worried that the merger would restrict consumer choice in relation to privacy and concluded that data privacy could be negatively affected by the merger.[64] Nevertheless, the Commission allowed Microsoft to acquire LinkedIn with the condition that they comply with a series of commitments that would address competition concerns raised by the Commission.

56 Jörg Hoffmann and Germán Johannsen, "EU-Merger Control & Big Data on Data-specific Theories of Harm and Remedies," *Max Planck Institute for Innovation & Competition* (2019): 15.

57 Ibid.

58 *European Commission Decision of Microsoft/LinkedIn Case*, para. 1.

59 Ibid., paras 176-181.

60 Ibid., para. 179.

61 Ibid., para. 180.

62 Ibid., fn. 330.; Directorate-General for Competition, European Commission, *European Commission Decision of Facebook/Whatsapp Case*, October 2, 2014, Case No. COMP/M.7217, paras 87, 102, fn. 79.

63 *European Commission Decision of Facebook/Whatsapp Case*, fn. 79.

64 *European Commission Decision of Microsoft/LinkedIn Case*, paras 351-352.

Competition in the European Union in the Digital Economy and Society

The ECJ *Meta* and the *Microsoft/LinkedIn* Cases are significant because they highlight how the economy and society has transformed with regards to using data. As the Court of Justice in the ECJ *Meta* Case noted:

> *[E]xcluding the rules on the protection of personal data from the legal framework to be taken into consideration by the competition authorities when examining an abuse of a dominant position would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union.*[65]

The European Commission's decision in the *Microsoft/LinkedIn* Case underscored a competition authority's consideration for data and privacy in competition assessments even for mergers and acquisitions. Competition authorities must consider practices surrounding data in this new digital age.

Considerations for Cambodian Competition Assessment in the Digital Age

While the EU has taken the charge in enforcing competition rules with consideration for data privacy, Cambodia is in the early stages of competition regulation. Nevertheless, it possesses tools to address data and privacy concerns in competition in the digital age. This Section will examine the applicability of the EU's consideration for data and privacy in competition assessments within Cambodia's legal framework.

An innovative approach to competition is required due to the complexity of digitalization.[66] How consumers' personal data are being collected and processed affects their right to privacy. Naturally, privacy should be seen as part of consumers' welfare. Because the Law on Competition focuses on consumer welfare,[67] privacy and data protection should be considered in Cambodian competition assessments.

The CCC may, under the Law on Competition, assess whether a firm is abusing its dominant position,[68] or whether the merger is anti-competitive,[69] except if the firm is in the telecommunications sector. In such case, as discussed in Section II, MPTC and TRC would be the entities conducting such assessments.[70] Applying the ECJ *Meta* Case and the *Microsoft/LinkedIn* Case, if a competition assessment is being conducted on a company within the telecommunications sector, MPTC and TRC, (not the CCC), can collaborate with the data protection authority to determine whether the company's conduct complies with data protection rules, in the context of both an abuse of domination and merger and acquisition.

Within the ICT sector, the Law on E-Commerce and the Sub-Decree on the Authorization for Operation in the ICT sector do not explicitly mention competition regulation. Nevertheless, MPTC is the leading ministry in digital transformation and digital government, and it is the ministry that regulates ICT.[71] A competition assessment requires specific and detailed knowledge of

65 *Meta Platforms Inc and Others v Bundeskartellamt*, para. 51 (emphasis added).

66 "Competition Assessment Toolkit," *OECD*, accessed September 24, 2023, https://www.oecd.org/competition/assessment-toolkit.htm.

67 Law on Competition, art. 1.

68 Law on Competition, arts 9-10.

69 Law on Competition, art. 3.

70 Law on Telecommunications, chap. 10.

71 "Cambodia Digital Economy and Society Policy Framework 2021-2035;" "Cambodia Digital Government Policy 2022-2035;" Law on E-Commerce, art. 26; Sub-Decree No. 110 ANKR.BK.

the industry. No other Cambodian ministry or institution is equipped or has the resources to make an adequate competition assessment within the ICT industry. Moreover, due to the rapid evolution of technology, telecommunications and ICT are approaching convergence.[72] Whether or not MPTC and TRC will be the sole competition regulator of firms within the ICT sector will be a policy decision. Nevertheless, for the reasons mentioned above, MPTC and TRC are critical establishments and must be involved in competition assessments in the ICT sector.

In other sectors where the CCC has authority, the approach by the Court of Justice in the ECJ *Meta* Case may be adopted. The CCC would consult and cooperate with the data protection authority, while observing their respective powers and competences. The data protection authority can evaluate and decide whether data protection rules were infringed. The CCC can rely on such findings to assess whether the conduct by these firms is an abuse of dominant position or whether the merger and acquisition is anti-competitive.

Conclusion and Recommendations

Many countries and regions, especially the EU, have integrated data privacy into their competition assessment. Privacy and data protection concerns not only have a significant impact on consumers but are also tied to competition. Technology companies engage in fierce competition to obtain that competitive edge, motivating them to collect and process nearly unlimited amounts of data. Such practices, particularly when they are in a dominant position, may lead to abuse, harming not only the users but also fair and honest competition in the market. Similarly, in certain mergers between data-driven firms, the merged entity may possess such data concentration that would expand its market power and increase barriers to its competitors who need access to such data to properly compete. These cases from the EU can assist Cambodia in preparation for its digital transformation. Cambodia, one of Southeast Asia's fastest growing economies, has made significant strides in both digital transformation and competition, and it will need to adopt an innovative approach to competition in the digital age. Cambodia can apply these practices from the EU within Cambodia's context—the particularities will depend on the sector, but in general the competition authority may take into account privacy and data protection violations to assess whether the conduct or merger and acquisition is anti-competitive. In doing so, the competition authority shall collaborate and at times defer to the data protection authority, especially on matters of privacy and personal data protection violations.

72 Ivan Huang et al., "The Convergence of Information and Communication Technologies Gains Momentum," *World Economic Forum*, 2012, https://www3.weforum.org/docs/GITR/2012/GITR_Chapter1.2_2012.pdf.

Personal Data Protection

Blockchain Technology and Personal Data Protection for Cambodia: Personal Data, Data Controller, and Right to Be Forgotten

Phan Daro

Abstract

This article explores the challenges posed by blockchain technology to personal data protection principles in the General Data Protection Regulation. The discussion shows how blockchain's features could potentially undermine conventional data protection paradigms with regard to personal data, data controller, and "right to be forgotten". The article also underlines the need for innovative personal data protection legislation in Cambodia that reconciles technological advancement with the protection of personal data.

Introduction

The adoption of blockchain technologies is predicted to provide enormous economic value, with estimates predicting that blockchain technology might add up to $1.76 trillion to the global GDP by 2030.[1] Similarly, it is also estimated that three quarters of the world population will have their personal data protected under modern privacy laws by the end of 2024.[2] What do these estimations mean for legal practitioners and blockchain-based application developers, especially for Cambodia? One implication might be that there are legal and technological challenges for both of them. On the one hand, legal practitioners have to decide whether or not metadata and public key shared among blockchain nodes are personal data in light of the available technological and legal means. On the other hand, blockchain-based application developers may be limited by the features of blockchain technology to comply with the law if data subjects want to enforce the "right to erasure" or "right to be forgotten". Additionally, who determines the purposes and means of data processing in the case of blockchain technology?

This section begins by briefly explaining the concepts of blockchain technology and personal data protection. After exploring the relationship between blockchain technology and personal data protection, it highlights the legal concerns regarding what constitutes personal data, who data controller is, and how the "right to be forgotten" be enforced.

Concept of Blockchain Technology

At its core, blockchain refers to a decentralized and immutable digital ledger that records transactions across several computers.[3] The transactions stored in the decentralized and immutable ledger could be any information that contains the details of every activity.[4] These transactions are then packed into blocks which are linked in chronological order, and copies of the ledger are hosted on multiple nodes in the network.[5] There are three main types of blockchain.[6] The first type is known as public blockchain. It is also called permissionless because data recorded on the public blockchain is open and accessible by everyone who operates a node,

1 PricewaterhouseCoopers, "Blockchain Technologies Could Boost the Global Economy US$1.76 Trillion by 2030 through Raising Levels of Tracking, Tracing and Trust.," PwC, accessed August 18, 2023, https://www.pwc.com/gx/en/news-room/press-releases/2020/blockchain-boost-global-economy-track-trace-trust.html.

2 "Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner, accessed February 25, 2024, https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024.

3 For technical overview of blockchain technology, see David L. Shrier, Basic Blockchain: What It Is and How It Will Transform the Way We Work and Live (London: Robinson, 2020); "Guide on Personal Data Protection Considerations for Blockchain Design" (Personal Data Protrection Commission Singapore, 2022).

4 Deeksha Dabas and Hitesh Bhatt, "Trajectory of Blockchain Technology in India: From Use Cases to Data Protection Regime," SSRN Scholarly Paper (Rochester, NY, March 3, 2022), 70, https://papers.ssrn.com/abstract=4200987.

5 This decentralized and immutable digital ledger is supposed to assure transparency, accountability, and security. See Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code (Cambridge, MA: Harvard University Press, 2019), 13.

6 For further detailed explanation of blockchain technology, see Jean Bacon et al., "Blockchain Demystified," SSRN Scholarly Paper (Rochester, NY, December 20, 2017), https://papers.ssrn.com/abstract=3091218.

with read and write permission, on that blockchain network.[7] The second type is called private or permissioned blockchain. In permissioned blockchain, there must be an authorization from an administrator for someone to operate a node on the private blockchain. Only one administrator who is the owner of the blockchain has the capacity to read and write transactions.[8] The last one is known as hybrid blockchain or consortium blockchain. This hybrid blockchain is governed by a restricted group of administrators who have agreed to create terms regulating consensus. Only selected users who have been authorized have the capacity to write transactions while reading permissions can be specified as either public or private.[9] Both permissionless and permissioned blockchain technologies pose challenges in determining data controllers since data on blockchain is distributed across multiple nodes. Furthermore, data stored on blockchain is also immutable, meaning that it is difficult, if not impossible, to remove the data from the blockchain.

Concept of Personal Data Protection

Personal data protection law, generally, aims to protect personal privacy by regulating the collection, processing, disclosing, and transferring of personal data. In ASEAN, there is ASEAN Framework on Personal Data Protection (ASEAN FPDP) which establishes principles and rules for member governments to secure data protection.[10] The ASEAN FPDP shares similar principles of the General Data Protection Regulation (GDPR).[11] Both frameworks emphasize concepts such as accountability, informed consent, and individuals' rights over their personal data. For the sake of the discussion, this article looks at three aspects of personal data protection. First, what constitutes personal data. Typically, personal data refers to any information that relates to an identified or identifiable individual. This broad category includes a variety of data, ranging from basic identifiers like names and contact details to more sensitive information such as biometric data and financial records. The second aspect is data controller. Most personal data protection laws presume that either a controller, processor, or both are present wherever personal data is processed. Third, the "right to erasure" or "right to be forgotten" grants individuals the right to request the deletion of their personal data when it is no longer necessary for the original purpose or when consent is withdrawn. These aspects of personal data protection appear to be in opposition to the decentralized and immutable characteristics of blockchain technology.

Relationship between Blockchain Technology and Personal Data Protection

With these basic concepts, there seems to emerge the relationship or potential tensions between three aspects of personal data protection and features of blockchain technology. First, if the data stored on blockchain-based applications meets the legal definition of personal data, the blockchain technology must comply with all the requirements of the law. Nevertheless, this article delves into more than typical direct personal data as it investigates the "metadata" and public key that blockchain technology employs to enable a decentralized function.[12] Second, most personal data

7 Diogo Duarte, "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR," SSRN Scholarly Paper (Rochester, NY, September 30, 2019), 15–19, https://doi.org/10.2139/ssrn.3545331.we provide a brief overview of blockchain technology from a legal perspective and its legal tensions with the General Data Protection Regulation (GDPR

8 Duarte, 19–20.we provide a brief overview of blockchain technology from a legal perspective and its legal tensions with the General Data Protection Regulation (GDPR

9 Noah Walters, "Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance," SSRN Scholarly Paper (Rochester, NY, April 20, 2019), 6–9, https://papers.ssrn.com/abstract=3481701.

10 ASEAN TELMIN, "Framework on Personal Data Protection" (ASEAN Telecommunications and Information Technology Ministers Meeting, 2016).

11 For a summary of GDPR, see "GDPR Summary," GDPR Summary (blog), accessed August 18, 2023, https://www.gdprsummary.com/gdpr-summary/.

12 Duarte, "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR," 31.we provide a brief overview of blockchain technology from a legal perspective and its legal tensions with the General Data Protection Regulation (GDPR

protection laws, in particular GDPR, operate under the implicit assumption that data is centralized and under the control or processing of identifiable actors. On the contrary, data controllers are not easily determined because blockchain-based applications are designed to operate in a decentralized manner, with multiple actors and participants within a widely distributed network. Third, personal data protection laws generally also assume that individual's personal data can be erased in any case, to comply with the legal requirements set under the law.

Legal Issues Concerning Blockchain Technology and Personal Data Protection

These relationships give rise to several legal concerns, which led to the idea that personal data protection principles are incompatible with blockchain technology's features. To understand these tensions, this article attempts to examine the key features of blockchain technology that pose challenges to personal data protection principles in GDPR. Through an analysis of the relationship between blockchain technology and principles governing the protection of personal data, this article makes a valuable contribution to the ongoing digital transformation in Cambodia as the country is preparing personal data protection law.

Contemporary Legal Framework on Personal Data Protection

This section begins with a summary of Cambodian laws and regulations pertaining to data protection and privacy. Following the summary of the Cambodian legal framework, it then highlights GDPR's provisions with respect to personal data, data controller, and "right to be forgotten".

Protection of Data and Privacy in Cambodia

Cambodia acknowledged the increasing importance of personal data protection in the digital era. The Ministry of Post and Telecommunications has begun drafting a personal data protection law, intending to govern the collecting, processing, and use of personal data by public and commercial organizations.[13] Some aspects of personal data may be protected under the Constitution, Civil Code, E-Commerce Law, and industry-specific laws despite that there are no clear definitions or obligations for personal data, data controllers or data processors and no specific authorities for data protection matters.

The 1993 Constitution generally acknowledges the privacy rights of the citizens. Article 40 of the Constitution guarantees Cambodian citizens the right to privacy in their homes and to keep their mail, telegrams, faxes, telexes, and telephone conversations confidential. Besides, an individual's personal data may be protected under the 2007 Civil Code as part of "personal rights" which include the right to privacy and other personal benefits and interests.[14] Article 12 of the Civil Code states that when the effects of an infringement of a personal right continue to exist, the owner of the right may seek the elimination of such effects. In the data privacy context, this legal provision potentially means that a person can seek an order to remove, for example, any storage of his or her personal data collected unlawfully.[15]

The E-Commerce Law, which was enacted in 2019 and entered into effect in 2020, controls all commercial and civil acts, documents, and transactions completed via an electronic system, except those pertaining to powers of attorney, wills and succession, and real estate.[16] Under

13 See "Cambodia to Strengthen Personal Data Protection Measures - Khmer Times," April 24, 2022, https://www.khmertimeskh.com/501063124/cambodia-to-strengthen-personal-data-protection-measures/.

14 Civil Code. Art. 10. 2007. (Cambodia)

15 Jay Cohen, Pichrotanak Bunthan, and Marina Sar, "Cambodia - Data Protection Overview," DataGuidance, September 7, 2021, https://www.dataguidance.com/notes/cambodia-data-protection-overview.

16 Law on Electronic Commerce (E-Commerce Law). Art. 3. 2019. (Cambodia)

the E-commerce Law, any person who privately maintains electronic data must establish all necessary means to ensure that the data is reasonably protected from loss, unauthorized access, use, alteration, leakage, or disclosure.[17] In addition, anyone who mistakenly enters the erroneous details into an automated system must be allowed to modify or remove the data, unless they have benefitted or caused damage to others by submitting the inaccurate information.[18]

Law on Banking and Financial Institutions, promulgated in 1999, is the main law governing entities licensed by the National Bank of Cambodia (NBC) to perform banking operations in the country.[19] It prevents anyone who participates in the administration, direction, management, internal control, or external audit of a covered entity, and employees of the latter, from providing confidential information pertaining to statements, facts, acts, figures, or the contents of accounting or administrative documents.[20] Prakas on Credit Reporting also regulates consent and data retention issues, requiring that consumer consent be obtained in advance if data will be used for anything other than the permitted purposes.[21] Banks and financial institutions should retain records, documents, and copies of documents involved in all forms of transactions for at least five years after the date of the transaction, and all data on a customer must be maintained for at least five years after the accounts have been closed or the business relations with the customer have ended.[22]

The Sub-Decree on the Code of Medical Ethics requires medical professionals and their staff to maintain patient confidentiality, and physicians may only provide essential information and documents regarding treatment to other medical professionals involved in treating the patient, or to those professionals that the patient chooses for a consultation, and only with the patient's consent.[23]

The Law on Telecommunications was enacted on December 17, 2015 and gives telecom subscribers the right to privacy, security, and safety in using telecommunications services, unless as otherwise stipulated by other laws.[24] The Telecom Law does not contain any particular data breach provisions or prohibitions on data transfer, nor does it clearly require data retention.

Overall, these laws generally recognize the right of individuals to their privacy, confidentiality, personal rights, which include their name, image, reputation, and privacy. However, there are no clear definitions or obligations for personal data, data controllers, or processors, and no specific enforcement or oversight authority for data protection issues. If blockchain technology is being utilized in any of the relevant sectors above, legal consultation must be taken with regard to, for example, the type of data that would be stored on the blockchain.

General Data Protection Regulation

As Cambodia has not yet adopted personal data protection law, a summary of GDPR's provisions with regard to personal data, data controller, and "right to be forgotten" helps shape the focus of this article. GDPR entered into force in 2016 and became legally binding in 2018. GDPR introduces data protection rights and obligations and enforces a data protection by "data protection by design and by default" approach. Article 4 (1) of GDPR defines "personal data" as

17 Law on Electronic Commerce (E-Commerce Law). Art. 32.
18 Law on Electronic Commerce (E-Commerce Law). Art. 18.
19 Law on Banking and Financial Institutions. Art. 1, 6. 1999. (Cambodia)
20 Law on Banking and Financial Institutions. Art. 47.
21 Prakas on Credit Reporting. Art. 9. 2020. (Cambodia)
22 Prakas on Anti-money Laundering and Combating the Financing of Terrorism. Art. 22.1. 2008. (Cambodia)
23 Sub-Degree on Physicians' Code of Ethics. Art. 4, 70. 2003. (Cambodia)
24 Law on Telecommunications (Telecom Law). Art. 65. 2015. (Cambodia)

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

Under GDPR, personal data refers to any information that relates to an identified or identifiable individual. It encompasses a broad range of data, from basic identifiers like names and contact details to more sensitive information such as biometric data and financial records.[25] In practice, there are two main types of personal data. First, direct personal data is data that can be attributed directly to a specific data subject without the use of additional information. For instance, the data's subject photo, DNA, or fingerprints. These types of data when stored on blockchain will be subject to personal data protection laws. Second, indirect personal data is data that can be linked to a specific data subject using additional information. For instance, the number plate of a car is indirect personal data, because it is possible to trace the car to its owner using additional information.[26] Pseudonymized data is a kind of indirect personal data, where the additional data required to identify the data subjects (the pseudonym), is only available to the controller. As some have noted pseudonymized data on a person is considered indirect personal data because identification is still technically possible.[27] Pseudonymized data is relevant here because the data stored on blockchain is not in plain text but rather encrypted or even hashed.

Data controllers play a crucial role in the application of GDPR. To understand the obligations of a controller on blockchain network, it is necessary to understand who is a controller. Article 4 (7) defines "controller" as

> *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

By definition, the one who determines the purpose and the means of the processing is the controller. A processor processes personal data on behalf of and under the direction of the controller. GDPR imposes obligations on identified controllers and processors. Nonetheless, identifying a controller or a processor in blockchain-based applications is not straightforward because every participating node has a copy of the ledger on its computer.

GDPR also gives rights to data subjects to have control over their personal data. Data subjects have the right to have their data "erased" in certain cases. Article 17 of GDPR states that

25 Leo Besemer, Privacy and Data Protection Based on the GDPR: Understanding the General Data Protection Regulation (Van Haren Publishing, 2020).2020

26 Besemer, 48.organizations collect and process personal data on a large scale. Free flow of data across Europe is vital for the common market, but it also presents a clear risk to the fundamental rights of individuals. This issue was addressed by the Council of the European Union and the European Parliament with the introduction of the General Data Protection Regulation (GDPR

27 Besemer, 48–49.organizations collect and process personal data on a large scale. Free flow of data across Europe is vital for the common market, but it also presents a clear risk to the fundamental rights of individuals. This issue was addressed by the Council of the European Union and the European Parliament with the introduction of the General Data Protection Regulation (GDPR

> *The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay (…)*

The "right to be forgotten" enables the data subjects to interfere with the processing of their personal data and revoke their consent with respect to such processing and demand to obtain deletion of their data without any undue delay when the requirements in Article 17 are met. For instance, when data is no longer necessary for collecting/processing purposes, the data subject can exercise the "right to be forgotten". However, the decentralized and immutable features of blockchain technology seem to conflict with the right "to be forgotten" of GDPR.

Personal Data Protection and Blockchain Technology for Cambodia

The discussion in this section with regard to personal data, data controller, and "right to be forgotten" provides some considerations for Cambodia to deal with blockchain technology and its future personal data protection law. As shown above, legal framework pertaining to personal data protection in Cambodian is still limited; as a result, the principles of GDPR are used for the discussion. Furthermore, this section also highlights two blockchain-based applications in Cambodia: Bakong app and *Verify.gov.kh.*

Blockchain Solutions in Cambodia: Bakong and Verify.gov.kh

Because of the decentralized and immutable characteristics of blockchain technology, Cambodia has also utilized this technology in various sectors. Two popular blockchain-based applications are discussed in this article. First, Bakong is a blockchain-based payment system, developed by the National Bank of Cambodia to streamline crossing-baking transactions. Bakong offers secure, real-time, and cost-effective peer-to-peer transfers and transactions, decreasing the need for traditional payment systems.[28] As a result, Bakong has contributed to enhancing financial inclusion, particularly in rural and underserved areas, by giving access to digital payment options to a wider audience. This article also found that the company behind Bakong uses Hyperledger Iroha which is a permissioned blockchain and distributed ledger.[29] However, the type of data which is processed on this permissioned blockchain is not publicly disclosed. As discussed below, the identification of data controllers in permissioned blockchain can also be controlled.

Second, Verify.gov.kh is an innovative online platform developed by Ministry of Post and Telecommunications. The platform allows users to validate the authenticity of government-issued documents by scanning a standard QR code affixed to the document. One of the key features of Verify.gov.kh is its integration of blockchain technology. This article found that the platform makes use of the permissionless Ethereum blockchain.[30] Permissionless blockchain raises several concerning issues with data controller and the "right to be forgotten," as will be seen in the discussion that follows. All of the new blockchain solutions in Cambodia must guarantee compliance with the country's future regulations regarding the protection of personal data.

28 National Bank of Cambodia, "Project Bakong: Next Generation Payment System" (National Bank of Cambodia, 2020), 20.

29 "SORAMITSU — Designing a Better World Through Decentralized Technologies," accessed March 3, 2024, https://soramitsu.co.jp.

30 The author confirmed with one of Verify.gov.kh team, saying that the platform uses Ethereum and Polygon blockchains. For Polygon, see "Polygon Labs Core Policy Principles," accessed March 3, 2024, https://polygon.technology/blog/polygon-labs-core-policy-principles.

Personal Data on Blockchain

The type of data stored on either permissionless or permissioned blockchain is of great importance because it determines the applicability of personal data protection law. If data stored on blockchain is direct personal data, the personal data protection law is applicable. However, this article attempts to highlight two types of data, metadata and public key, for consideration because there are still debates among legal practitioners in different jurisdictions whether these data are considered as personal data.[31] Metadata and public keys are distributed to all participating nodes in either permissionless or permissioned blockchains. At first, these types of data seem non-personal data. Nonetheless, the definition of personal data under GDPR is broad including indirect data which refers to any data that could be linked with other data to identify the data subject. Furthermore, public key in one sense is similar to an IP address. While there are no law cases on metadata or public keys as personal data, there are some discussions that highlight that IP addresses are considered personal data in some jurisdictions.[32] The Court of Justice of the European Union (CJEU) stressed that an IP address, even if it might not immediately identify an individual by itself, might become personal data if there is a legal way to link it to an identified person. The Court recognized that in circumstances when an Internet Service Provider contains extra information that can be used to identify the user linked with a given IP address, the IP address is definitely constituted personal data.[33] In case of blockchain, if metadata and public keys together with other publicly available data lead to an identified person, they should be considered as personal data. If Cambodia considers a broad definition of personal data, metadata and public keys pose the risk of unintended disclosure of personal data when it is combined with other readily available information. In fact, there is also discussion about the possible identification of person using the public key, IP address, and other patterns associated with those public keys.[34] For Cambodia, both legal practitioners and blockchain-based application developers have to be mindful with regard to these types of data because there might be a way in the future to use these types of data together with other pieces of information to identify an individual.

Another point relevant to personal data for Cambodia to consider is pseudonymity. For GDPR, the distinction between when a piece of data is considered pseudonymous or anonymous is vital in establishing GDPR's applicability. Under GDPR, pseudonymity "*means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".[35] The data on the blockchains, which are encrypted, are and will be pseudonymous within the meaning of the GDPR.[36] Hence, just because personal data are not in plain text does not mean it is outside the scope of personal data protection law. Finally, personal data should only be written on blockchain if consent for public disclosure has been obtained from the concerned individuals or if the personal data is already available publicly.

31 Claudia Martorelli, "GDPR and Ethereum Blockchain: A Compatibility Assessment," Trento Student Law Review 4, no. 1 (April 30, 2022): 109–13, https://doi.org/10.15168/tslr.v4i1.2194.

32 Normann Witzleb and Julian Wagner, "When Is Personal Data 'About' or 'Relating To' an Individual? A Comparison of Australian, Canadian and EU Data Protection and Privacy Laws," SSRN Scholarly Paper (Rochester, NY, February 1, 2018), https://doi.org/10.2139/ssrn.3189376.\\uc0\\u8221{} SSRN Scholarly Paper (Rochester, NY, February 1, 2018

33 Witzleb and Wagner, 16–17.

34 Cagla Salmensuu, "The General Data Protection Regulation and the Blockchains," SSRN Scholarly Paper (Rochester, NY, January 1, 2018), 19–22, https://papers.ssrn.com/abstract=3143992.

35 Besemer, Privacy and Data Protection Based on the GDPR, 119.

36 Primavera De Filippi, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies," Journal of Peer Production, no. n.7 (September 14, 2016): 11–12, https://papers.ssrn.com/abstract=2852689; Martorelli, "GDPR and Ethereum Blockchain," 109.

Data Controller on Blockchain

Under the GDPR, controlling the data means making a decision about why and how a particular data processing activity takes place.[37] Blockchain's decentralized nature can complicate the identification of data controllers because all participating nodes in blockchain not only process data but also store a copy of the data.[38] With regard to players in a blockchain, there are core developers, node operators, miners, and applications developers.[39] In the case of blockchain technology, who determines the purposes and means of data processing?

In a permissioned blockchain system, it is easier to identify a data controller even if the blockchain system is decentralized in nature as there is an administrator involved in such a blockchain system who determines the means and purpose of the processing of personal data.[40] Having said that, a permissioned blockchain should establish contractual controls; for example, there should be terms and conditions of use and access to participants.

However, many participants validate transactions in a permissionless blockchain network. Identifying a single entity as the data controller is complex, potentially hindering individuals' ability to exercise their rights. The lack of an identifiable entity or entities in the position of control on the permissionless blockchain applications is a feature of this technology.[41] This situation is likely to yield an accountability gap which is not ideal for the regulators or citizens. However, there are some suggestions for determining the data controller on blockchain.[42] As some have noted, the control should be shared among all nodes, and that all participants, particularly those that can be identified and located, are considered jointly and severally liable.[43] With permissionless blockchain, regulators and authorities will be challenged with the lack of an identifiable entity making decisions about how the data will be processed. For Cambodia, it should be noted that most personal data protection laws are not designed to serve a world where data is processed without anyone unidentifiable processing it.

Immutability of Blockchain and Right to Be Forgotten

Blockchain's immutability is another challenge for personal data protection compatibility. This immutability feature is a cornerstone of blockchain's security. Meanwhile, the "right to be forgotten" in most personal data protection laws requires data controllers to be able to remove personal data when it is no longer necessary for the original purpose or when consent is withdrawn, or as one of the conditions required is met.[44] The CJEU stressed the need to adopt a case-by-case approach when balancing clashing interests, taking into account the nature and the sensitivity of the information in question and the interest of the public in accessing it.[45] The inherent immutability of blockchain's core attribute really poses challenges in fulfilling the "right to be forgotten", where data removal contradicts the preservation of the historical accuracy of records. However, it is possible to disable access (read and write) to the data on the block from a technical point of view. As some have noted, the question is whether the "disabling access of others" will amount to "erasure" at law.[46] Besides, there are some discussions that blockchain

37 Besemer, Privacy and Data Protection Based on the GDPR.

38 Shikha Mishra, "Role of Controllers in the Realm of Decentralised Blockchain Technology and GDPR," SSRN Scholarly Paper (Rochester, NY, August 31, 2019), 27–28, https://papers.ssrn.com/abstract=3469189.

39 Martorelli, "GDPR and Ethereum Blockchain," 117–20.

40 Mishra, "Role of Controllers in the Realm of Decentralised Blockchain Technology and GDPR," 28.

41 Matthias Berberich and Malgorzata Steiner, "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers," European Data Protection Law Review (EDPL) 2 (2016): 422.

42 Gabriel Jaccard, "GDPR & Blockchain: The Swiss Take," SSRN Scholarly Paper (Rochester, NY, December 4, 2018), 12–13, https://papers.ssrn.com/abstract=3575231.

43 Henry Chang, "Is Distributed Ledger Technology Built for Personal Data?," SSRN Scholarly Paper (Rochester, NY, February 1, 2018), 8, https://papers.ssrn.com/abstract=3137606.

44 Besemer, Privacy and Data Protection Based on the GDPR.

45 Martorelli, "GDPR and Ethereum Blockchain," 138.

46 Cagla Salmensuu, "The General Data Protection Regulation and the Blockchains," SSRN Scholarly Paper (Rochester, NY, January 1, 2018), 23–27, https://papers.ssrn.com/abstract=3143992.

operators and participating organizations can comply with correction and retention limitation obligations by mandating secure disposal of the decryption keys of outdated data by other participants.[47] Furthermore, in terms of technology solutions, there is a project in the EU that is said to meet the "right to be forgotten" of GDPR.[48] In Cambodia, provisions related to removal or correction in the industry-specific laws could potentially provide a legal basis for a person to seek an order to remove any storage of his or her personal data collected unlawfully. However, data stored on a blockchain cannot be easily altered or erased without compromising the integrity of the entire blockchain.

Conclusion and Recommendations for Cambodia

Cambodia will have personal data protection law which reflect some of the ideas in GDPR. At the same time, blockchain technology will continue to be expanded to other sectors in Cambodia. Regulating such decentralized and immutability technologies is problematic for both developed and developing countries. The discussion above has shown that personal data protection laws apply to blockchain technology in most cases. The issues highlighted by the discussion, which give rise to the notion of incompatibility between personal data protection law and blockchain technology, relate to three aspects: the determining of personal data, the identification of data controller, and the enforcement of "right to be forgotten". Blockchain-based application developers should be mindful and should work with personal data protection legal practitioners when designing and developing blockchain-based applications to minimize the impact stemming from the incompatibility issues. One possible way is to design the applications such that no personal data controlled by participating organizations is written on-chain either in cleartext, encrypted, or anonymized forms. Similarly, participating organizations should avoid business use cases that require uploading any personal data on-chain in clear text, encrypted, or anonymized forms onto a permissionless blockchain. They can instead consider off-chain approaches that store personal data in centralized data repositories, while only writing representations of the personal data on-chain. Such an off-chain approach can thus be used to fulfill personal data protection obligations in both permissionless and permissioned networks.

As Cambodia is preparing personal data protection law, the following recommendations could enhance the balance between technological innovation and personal data protection rights. First, the law should emphasize the exploration of off-chain solutions within blockchain applications involving personal data. Storing sensitive data off-chain while using blockchain for verification could facilitate data removal without compromising the core structure of the blockchain. Second, the principles of data minimization and purpose limitation should be integral to Cambodia's personal data protection law. Encouraging organizations to collect only the necessary data for a specific purpose minimizes the need for data removal requests. Third, Cambodia could advocate for robust consent management mechanisms. These mechanisms should empower data subjects to manage their data, including modification or withdrawal of consent, even within immutable systems. Additionally, a "right to explanation" could be incorporated into the law. This ensures that individuals understand how their data is processed and why specific information is retained, even within systems where erasure is challenging. Furthermore, Cambodia should require organizations to communicate clearly with individuals about the purposes and methods of data processing, ensuring informed consent. This will build trust and empower individuals to exercise control over their personal data. Finally, Cambodia's law could establish criteria for determining joint data controller status. In situations where multiple entities are involved in data processing, clear guidelines can ensure that each entity understands its specific responsibilities and liabilities. In short, blockchain technology falls within the purview of personal data protection legislation. The compatibility issues mentioned can be resolved as both blockchain technology and the legislation are advancing. Legal practitioners and blockchain-based application developers should collaborate to use the technology's benefits for the general public.

47 Salmensuu, 23–25; Chang, "Is Distributed Ledger Technology Built for Personal Data?," 3–4.

48 Giovanni Maria Riccio et al., "The POSEID-ON Blockchain-Based Platform Meets the 'Right to Be Forgotten,'" SSRN Scholarly Paper (Rochester, NY, 2020), https://doi.org/10.2139/ssrn.3745516.

Privacy and Data Protection

The GDPR and the Vietnamese Decree n°13/2023/ ND-CP: Comparative Analysis of a Recent Legal Framework in Southeast Asia Regarding the Personal Data Protection

Thomas Honnet

Abstract

After several years of drafting, negotiating and listening feedback, Vietnam finally adopted its new personal data protection regulations on April 17, 2023 and came into force on July 1, 2023 which is known as Decree n°13" on 17 April 2023. The decree was developed pursuant to the 2015 Civil Code, the 2004 Law on National Security, and the 2018 Law on Cybersecurity. This decree is aligned with an international framework (the guidelines of the United Nations[1], of the ASEAN[2], of the Convention 108+[3]) that shares common principles such as the need to have a legal basis for processing data, to clearly define and limit the purposes, to have a limited retention period, etc. It is also, obviously, part of a particular national framework, with very specific rules: no independent supervisory authority, existence of a list of "general data", etc. While some of these rules reflect the historical and sociological specificities of each country, others are more unconventional and demand detailed commentary.

Conducting a critical analysis of this new legal framework and comparing it with the General Data Protection Regulation (GDPR), recognized as being one of the most protective legal frameworks globally, though subject to its own criticisms, it will certainly be interesting for Cambodia to take a close look at this new regulation and this less new one (the GDPR came into force in 2018 but is very largely inspired by the French framework[4], in force since 1978), to draw inspiration from it. The purpose of the comparison is to understand the differences between the two countries' regulations, and to draw out the good and bad ideas, so that Cambodia will not make the same mistakes and will find its own way.

Introduction

Vietnam marked a significant step on 17 April 2023 by adopting its new personal data protection regulations, known as "Decree n°13".[5] In the today's digitized world, personal data protection regulations are becoming increasingly crucial, and governments worldwide have recognized their importance in safeguarding their citizens, facilitating international trade, and maintaining a global presence. The General Data Protection Regulation[6], renowned as one of the most protective legal frameworks globally, previously shed light on this international movement a few years ago. With this in mind, we find it valuable to compare these two legal frameworks to offer insights that Cambodia can consider, whether to draw inspiration or not, as it shapes its own regulations. This comparison is interesting because on one hand, the GDPR is the major standard in the world, on which all international common rules, but also all new national regulations, are based or at least strongly inspired, and on the other hand, Vietnam is the last country in Asia that have adopted a national regulation on personal data protection. So we will be able to see the similarities and differences, the influences, the specificities of a recent Asian example.

1 "Data Privacy, Ethics and Protection. Guidance note on big data for achievement of the 2023 Agenda": https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

2 "ASEAN Framework on Personal Data Protection" : https://www.dataguidance.com/legal-research/asean-framework-personal-data-protection

3 Convention 108+. Convention for the protection of individuals with regard to the processing of personal data: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

4 Law n°78-17 of January 6, 1978 on data processing, data files and individual liberties: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

5 Decree N° 13/2023/ND-CP.

6 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.

The RGPD is "directly applicable" in the internal legal order of the member states of the European Union, so it doesn't need any other internal texts to apply. Announced in 2016, Europeans knew that they would have to comply with all its rules from 2018, when it came into force. However, by 2018, very few companies had complied. Even worse, in 2024, many companies are still not complying with the rules, or are doing so poorly. Why? There are many reasons: national supervisory authorities can't control everyone; companies have other priorities, or not enough resources, or does not take care of it voluntarily; the rules are still poorly known and understood... In the event of an inspection, national supervisory authorities will often be sympathetic, supporting companies that have made an effort, and punishing those that have not: this is the accountability principle. It is still too early to say in Vietnam, but there is a good chance that it will be the same thing: all companies, all administrations, all associations process personal data. So how to do it? It takes time, understanding, support, education, but also harsh sanctions against those who voluntarily process data illegally. This is a balance that Cambodia will also have to find.

While both legal frameworks share common points that echo major international principles increasingly recognized by many (existence of a legal basis[7], of determined purposes[8], of a security obligation[9], or to have a processing register[10], to respect the right to information[11], etc.), there are slight differences that do not substantially alter the overall objectives. For instance, retention periods: in the GDPR[12], the data controller must determine, for each category of data, a maximum (and sometimes minimum) retention period. This period is either set by some national laws (for example, in France, you must keep all contracts concluded as part of a commercial relationship for five years[13]) or set by the data controller himself. If necessary, he must define a retention period according to the objectives pursued by the data processing, that is to say its purposes. In contrast, the Vietnamese decree[14] specifies that personal data should be stored for an appropriate period considering the processing's purposes, unless otherwise stipulated by law.

Despite these similarities, there are notable differences between the two regulations that deserve our attention.

This paper aims to explore and discuss these differences in depth. It is essential to emphasize that the objective is not to define regulations as "good" or "bad", but rather to offer a critical and practical perspective on what appears relevant and globally shared by many countries. While advocating for respect for national specificities and sovereignty, this paper aims to provide insights on essential aspects of personal data protection.

Regarding the methodology of this paper, we are therefore going to highlight several points that seem essential to us and analyse each of these points as follows:

- to present the legal framework and national policy,
- to analyse actual implementation and discuss competing solutions and challenges, and to provide recommendations for Cambodia.

7 Decree N° 13, articles 11 and 17; GDPR, article 6.
8 Decree N° 13, article 3.3; GDPR, article 5 b).
9 Decree N° 13, articles 26 and 27; GDPR, article 32.
10 Decree N° 13, article 38, GDPR, article 30.
11 Decree N° 13, articles 3 and 9, GDPR, articles 12, 13 and 14.
12 GDPR, article 5 e).
13 Commercial Code, article L110-4.
14 Decree N° 13, article 3.7.

Potential Guidance for Cambodia from Benchmarking GDPR and Vietnam's New Decree about Personal Data Protection

Since 1995, a European directive has regulated the legal framework for personal data protection in Europe[15]. While directives impose general common rules for all member States of the European Union, they also allow certain flexibility for each country to have its own national specifications. However, the GDPR, being a European *règlement*, is directly applicable in the national legal order of all member countries, imposing unified rules and leaving very few variations.

The new Vietnamese decree adds to an already fragmented legal framework[16], resulting in the absence of a clear, unified, coherent, and comprehensive law. This lack of clarity can lead to problems in understanding and legal certainty. For example, the rights of the persons concerned by data processing only exist at the level of decrees, which means at the regulatory level and not at the legislative level. An interesting example[17] of this is the unauthorized transfer or sale of personal data without the individual's consent (which is a bad idea: it's a good rule for sales, but it's definitely too strict for simple transfers that can simply take place between a data controller and its processor), which constitutes a violation of their rights[18]. However, Vietnamese law considers a transaction invalid only when it violates "the prohibition of the law"[19]. As a result, the prohibitions of the decree may not align with those of the "law" (even if paragraph 4 of article 3 of the Civil Code of 2015 stating that "the establishment, exercise, extinction of the rights and civil obligations shall not prejudice the national interests, the interests of ethnic groups, the public interests and the legitimate rights and interests of others": this last point would obviously be violated by a violation of the decree). Therefore, we believe it is important for Cambodia to establish a single legislative text that encompasses all data protection rules.

Consent is Not the Alpha and Omega of Personal Data Processing

The GDPR requires each processing operation to have a "legal basis"[20], i.e. a legal justification that "authorizes" the data controller to process the data. There are six different legal bases:

- The people's consent;
- A contract;
- A legal obligation;
- The safeguarding vital interests;
- A legitimate interest (which is difficult to apply to administrations);
- A public interest

It is similar in the Vietnamese decree, but the philosophy is not the same. Article 11 of the decree states "The consent of the data subject shall be granted to all activities in the processing of his/her personal data, unless otherwise provided for by law", and Article 17 (about "Personal data processing without the consent of data subject") states:

> *1. The personal data shall be processed to protect the life and health of the data subject or others in an emergency situation. The Personal Data Controller, the*

15 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

16 The cyber information security law no. 86/2015/QH13 of November 19, 2015, for instance, or cybersecurity law no. 24/2018/QH14 of June 12, 2018.

17 Highlighted during a symposium on May 25, 2023 in Hô Chi Minh-City on the protection of personal data, by Prof. Dr. *Đỗ Văn Đại* and Dr. Nguyễn Thị Hoa.

18 Decree N° 13, article 22.

19 Civil Code 2015, article 117 and 123.

20 GDPR, article 6.

> *Personal Data Controller-cum-Processor, the Personal Data Processor and the Third Party shall be responsible for proving such situation.*
> *2. Disclosure of personal data in accordance with the law;*
> *3. Processing of personal data by competent regulatory authorities in the event of a state of emergency regarding national defence, security, social order and safety, major disasters, or dangerous epidemics; when there is a threat to security and national defence but not to the extent of declaring a state of emergency; to prevent and fight riots and terrorism, crimes and law violations according to the provisions of law;*
> *4. The personal data shall be processed to fulfil obligations under contracts the data subjects with relevant agencies, organizations and individuals as prescribed by law;*
> *5. The personal data shall be processed to serve operations by regulatory authorities as prescribed by relevant laws.*

Vietnam's data protection system relies more on the "principle/exceptions" rule rather than on an initial choice between several equivalent legal bases. This is quite surprising, as it contradicts the common belief that the consent of the persons concerned is not the *alpha* and *omega* of data processing, even less for public administration and their public service missions (it's even not recommended by the GDPR itself, in its recital 43[21]). Therefore, when the processing is based on a public interest, it is inappropriate to ask for the "agreement" of the persons concerned to process their data. Consequently, they will not have the option to "withdraw" this consent since they never provided it in the first place. Therefore, it appears essential to us, for Cambodia, to have multiple legal bases and not to focus everything on the consent of individuals, which is not frequently used in reality.

An Independent Supervisory Authority

The GDPR firmly establishes the existence of an independent supervisory authority, separate from any government influence. The whole Chapter 5 is devoted to this idea. Article 52 provides details on this independence:

> *1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.*
> *2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.*
> *3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.*
> *4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.*
> *5. Each Member State shall ensure that each supervisory authority chooses and has its own staff, which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.*

21 "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."

> *6. Each Member State shall ensure that each supervisory authority is subject to financial control, which does not affect its independence, and that it has separate, public annual budgets, which may be part of the overall state or national budget.*[22]

It is important to note that Vietnamese decree differs significantly: there is no independent supervisory authority: the Government assumes the role of monitoring compliance with the law on the protection of personal data, is responsible for distributing guides on best practices and benchmarks, as well as penalizing entities that fail to comply with the regulations, etc.[23] Additionally, the Government (the Ministry of Public Security, specifically the Department of Cybersecurity and Hi-tech Crime Prevention) receives notifications of data breaches.[24]

However, the article 29 of the Decree still has provision on "specialized personal data protection authority and national portal on personal data protection" under which there are two entities:

- the agency in charge of personal data protection is the Department of Cybersecurity and High-Tech Crime Prevention and Control;
- the Ministry of Public Security, which is responsible for assisting the Ministry of Public Security and National Portal on Personal Data Protection (this one is competent to give a sanction for violation in personal data protection).

It is easy to understand why the idea of an independent supervisory authority is not suited to Vietnamese politics and society. However, this raises concerns. Data controllers are not only private actors, and the administration itself processes a large amount of citizen data to fulfil its public service missions. However, how to ensure compliance with the regulations by administrations if the administration controls itself? We recommend for Cambodia the establishment of an independent authority that can impartially control and provide recommendations freely to both public and private entities.

Performing a Privacy Impact Assessment (PIA): Never, Sometimes, Always?

In the GDPR, a Privacy Impact Assessment is a tool used to ensure data processing is compliant with the GDPR and respects individuals' privacy rights and freedoms, especially when the processing of personal data may create significant risks.

The PIA helps to identify and analyse potential risks associated with data processing, such as data destruction, data theft, etc. It also highlights the measures implemented to mitigate and eliminate these risks. Additionally, the PIA allows data controllers to assess certain risks that might be unlikely to occur or would not have severe consequences for the individuals affected by the data processing.

To determine whether a data controller should conduct a PIA, they should refer to three additional reading grids: the first one is the GDPR itself, which refers to processing "likely to create a high risk for the rights and freedoms of data subjects", and draws up a non-exhaustive list:

> *(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or*

22 GDPR, article 52.
23 Decree N° 13, article 5.
24 Decree N° 13, article 23.

similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) systematic monitoring of a publicly accessible area on a large scale.[25]

The second one is the national control authority, which can establish some lists of processing that must be subject to a PIA, or not be subject to a PIA[26].

The last one is the European Data Protection Supervisor (EDPS), which has set up a list of nine criteria. If the processing meets at least two of the nine criteria, a PIA must be carried out:

- Evaluation/scoring (including profiling);
- Decision with legal or similar effect;
- Routine monitoring;
- Collection of sensitive data or data of a highly personal nature;
- Collection of personal data on a large scale;
- Crossing;
- People (patients, elderly people, children, etc.);
- Innovative use (use of a new technology);
- Exclusion from the benefit of a right/contract.

Therefore, as we can see, the European framework is highly detailed. On the other hand, the Vietnamese one seems less accurate: the personal data controller has to do and store a dossier on the assessment of the impact of personal data processing from the time of starting to process personal data.[27] Additionally, if they intend to send personal data outside Vietnam, a separate dossier on the assessment of the impact of outbound transfer is required.[28] In these dossiers, they have to write all the following information: contact information and details of the Sender and the Receiver, full name and contact details of an organization or individual under the Sender involved in sending and receiving a Vietnamese citizen's personal data, description and explanation about objectives of the processing of a Vietnamese Citizen's personal data after the personal data is transferred abroad, assessment of impact of personal data processing; undesirable consequences and damage that may occur, measures for reducing or removing such consequences and damage, etc.

It is not uncommon for data protection frameworks to be complex and challenging to implement, and this can be particularly true for smaller businesses and organizations. When the requirements are overly burdensome, there is a risk that companies may not be able to comply fully, leading to potential violations of privacy rules. To address this issue and strike a balance between data protection and practicality, it may be reasonable for Cambodia to limit the PIA to specific scenarios where the processing of sensitive data or higher-risk data occurs.

With the Letter of the Text, Its Spirit: A Prior Formalities System or an Accountability System?

The GDPR has created a real shift in the philosophy of personal data protection in Europe, moving from a system of prior formalities to a regime of accountability. This change, in substance, consisted in making data controllers responsible, trusting them, while expecting them no longer

25 GDPR, article 35.
26 For instance, for the French one: https://www.cnil.fr/sites/cnil/files/atoms/files/liste-traitements-aipd-requise.pdf
27 Decree N° 13, article 24.
28 Decree N° 13, article 25.

to comply with prior formalities or upstream procedures, but to comply with the rules and keep documentation capable of proving this compliance.
Thus, in France for example, there were systems of advice from the supervisory authority, authorizations from the supervisory authority, issuance of a ministerial decree, simple decree, decree taken into Conseil d'Etat, etc.[29] (in reality, they are now limited to rare and very specific cases). Above all, no more "declarations": for the vast majority of data processing that did not require other formalities, declarations to the supervisory authority were necessary.[30] In 2018, the GDPR put an end to these systems and largely replaced them with a logic of documentation, accountability and trust: Records of processing activities[31], Data Protection Impact Assessment[32], Privacy by design[33], codes of conduct[34], certification mechanisms[35], prior formalities limited to the most sensitive cases, still requiring decrees issued by the Conseil d'Etat, with[36] the opinion of the authority supervisory authority, or even ministerial decrees after consulting the supervisory authority[37]).

The Vietnamese decree, if it forces data controllers to keep a Records of processing activities[38], has not made this changeover: for each data processing, it obliges data controllers to keep files on the assessment of the impact of personal data processing, which shall be always available in order to serve inspection and assessment by the Ministry of Public Security. In addition, the Ministry of Public Security shall receive one authentic copy of a declaration within sixty days from the date of processing of personal data.[39] Also, for each outbound transfer of personal data, the sender shall also send one authentic copy of a dossier on the assessment of the impact of outbound transfer of personal data to the Ministry of Public Security within sixty days[40] (the Ministry can ask more details and modifications). The sender is required to inform the Ministry of Public Security in writing about the data transfer, providing information on the transfer and the contact details of the organization or individual responsible for the transfer, once the personal data has been successfully transferred.

Why the GDPR changed the spirit of compliance? Three points were problematic: firstly, the supervisory authority obviously did not have the resources (human, time, financial) to read all the documents sent by millions of data controllers. Secondly, these preliminary procedures relieved the responsibility of data controllers: many data controllers believed that fulfilling these procedures excused them from their overall obligations under the GDPR. Lastly, all these procedures placed a considerable burden on data controllers. They perceived the requirements for personal data protection as a negative aspect, leading to dissatisfaction with the regulation. This is why it seems essential to us for Cambodia to opt for an accountability regime, to make the actors responsible and of course, in the event of control and non-compliance with the rules, to sanction them.

29 French Data Protection Act, old articles 25, 26, 27 and 29.
30 French Data Protection Act, old article 22.
31 GDPR, article 30.
32 GDPR, article 35.
33 GDPR, article 25.
34 GDPR, articles 40 and 41.
35 GDPR, article 42 and 43.
36 French Data Protection Act, article 30.
37 French Data Protection Act, article 31
38 Decree N° 13, article 38.
39 Decree N° 13, article 24.
40 Decree N° 13, article 25.

Other Less Important but Still Interesting Points

First point, the definition of personal data. In the GDPR, it's *"any information relating to an identified or identifiable natural person"*[41]. The definition is broad and makes it possible to include a great deal of data. Legally, we think that it is a good thing that the texts are general, which will allow the judges or other texts (decrees for example) to specify the notions. In the Vietnamese decree, two things draw our attention: on one hand, personal data refers to "electronic information in the form of symbols, letters, numbers, images, sounds, or equivalences associated with an individual or used to identify an individual. The personal data includes general personal data and sensitive personal data."[42] Here, the term "electronic" seems surprising to us because it is important not to make the mistake of believing that personal data only concerns the digital world. Of course, the digitization has amplified data flows and the risk of breach, but it seems important to us for Cambodia to have a single regulation on digital data and "physical" data, on paper for example.
Also: the Vietnamese decree gives examples, specifying the data concerned: "last name, middle name and first name, other names, date of birth; date of death or going missing; gender; (...)", but still including the "information associated with an individual or used to identify an individual". This point seems very important to us for Cambodia because it is essential not to have an exhaustive list of all the data, since the legislator will obviously forget certain situations because new technologies evolve very quickly.

Another element that seems interesting to us is about sensitive data. The GDPR and the Vietnamese decree provide definitions and examples, relatively comparable but with differences. It is above all their legal framework than their definitions that interests us. The GDPR prohibits the processing of this data, with the following exceptions[43]: the data subject has given explicit consent, processing is necessary to protect the vital interests of the data subject, processing relates to personal data which are manifestly made public by the data subject, etc. (there are about ten exceptions). The Vietnamese decree does not have this prohibition, and has a legal framework not really more protective than the one of "general" data[44]:

> *1. Adopt measures mentioned in Clause 2 Article 26 and Article 27 of this Decree.*[45]
> *2. Appoint a department with the function of protecting personal data and personnel in charge of protection of personal data, and exchange information about the department and individual in charge of protection of personal data with the personal data protection authority. Exchange information about the individual in charge of protection in case the Personal Data Controller, the Personal Data Controller-cum-Processor, the Personal Data Processor or the Third Party is an individual.*
> *3. Notify the data subject of the processing of his/her sensitive personal data, except for cases specified in Clause 4, Article 13, Article 17 and Article 18 of this Decree.*

It may seem surprising to us to create two different categories of data, and not to have such big differences in their protection. For Cambodia, we believe that a real, more protective and stricter framework is needed for sensitive data.

41 GDPR, article 4.
42 Decree N° 13, article 2.
43 GDPR, article 9.
44 Decree N° 13, article 28.
45 Which are "classic" security measures for all data actually.

Last interesting point: the age of consent for minors. It is sixteen years old in the GDPR[46], and seven years old in Decree No. 13[47]. It is difficult for us to have an opinion here, even if seven years old still seems very young: you must understand what it is about and have all the information on data processing to give your consent. For Cambodia, we recommend a minimum age of 15 or 16, to protect younger children.

Conclusion

The primary focus of this paper is not to criticize one regulation in favor of another or to present a single solution for Cambodia. Instead, its main goal is to conduct a comparative analysis of the two regulations and identify potential valuable insights and guidelines for Cambodia to consider. The paper's purpose is to initiate reflections and provide constructive remarks that Cambodian policymakers can use at their discretion. National data protection regulations require striking a delicate balance between adhering to major principles recognized by many countries and respecting the unique national and local specificities that enrich and define our diverse world. The ultimate intention is not to impose a universal approach, but to create doors which Cambodia can choose to open or not.

46 GDPR, article 8.
47 Decree N° 13, article 20.

Privacy and Data Protection

International Laws and European Data Protection: The Long Way to the GDPR and Ongoing Relations

Professor Federico Ferretti

Introduction

Historically, the primary object of data protection laws was identified with the protection of personal privacy within the context of processing operations involving personal data.[1]

More recently, dominant views have started seeing data protection as the protection through regulation of personal information pertaining to an identified or identifiable individual (data subject). Individuals do not own information about themselves and those who process personal data (data controllers and data processors) have the right to process data pertaining to data subjects as long as such processing is lawful, i.e. it abides to procedural rules set by a law whose objective is to protect individual citizens not against data processing per se, but against unjustified collection, storage, use, and dissemination of the data pertaining to them. According to this stance, data protection cannot be reduced to a late privacy spin-off echoing a privacy right with regard to personal data, but it formulates the conditions under which processing is legitimate. While privacy laws exist to protect the legitimate opacity of the individual through prohibitive measures, data protection forces the transparency of the processing of personal data enabling its full control by individuals where the processing is not authorised by the law itself as necessary for societal reasons. In short, data protection law focuses on the activities of the processors and it enforces their accountability, thus regulating an accepted exercise of power.[2]

Personal data processing operations are performed predominantly in large volumes with information and communications technologies. Data are increasingly processed over international electronic communications networks and across national and geographic boundaries.

Over time, these factors have encouraged the development of a harmonised European regulatory framework for data processing operations involving personal data, which has had impact further afield. Until May 2018, within the European Economic Area (EEA) the most important legal instrument was the Directive of the European Parliament and Council of 24 October 1995 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (the Data Protection Directive)[3]. With the ratification of the Treaty of Lisbon, Article 16 of the Treaty on the Functioning of the European Union (TFEU) has upgraded the provision on data protection to a 'provision of general application' under Title II alongside other fundamental principles of the EU. It also imposes on the EU legislator to establish a certain and unequivocal legal framework for data protection beyond the areas covered by what was covered by Pillar I (essentially, the internal market). Equally, the Charter of Fundamental Rights of the EU has become binding, which in its Article 8 recognises the protection of personal data as an autonomous right from privacy.

1 There is recognition of privacy in the Qur'an [an-Noor 24:27–28 (Yusufali); al-Hujraat 49:11–12 (Yusufali)] and in the sayings of Mohammed [Volume 1, Book 10, Number 509 (Sahih Bukhari); Book 020, Number 4727 (Sahih Muslim); Book 31, Number 4003 (Sunan Abu Dawud)]. The Bible has numerous references to privacy: see Hixson R, *Privacy in a Public Society: Human Rights in Conflict* (Oxford University Press, 1987); Moore B, *Privacy: Studies in Social and Cultural History* (Routledge, 1984). Jewish law has long recognised the concept of being free from being watched: see Rosen J, *The Unwanted Gaze: the Destruction of Privacy in America* (Random House, 2000). There were also protections in classical Greece and ancient China: see Smith RE, *Ben Franklin's Web Site* (Sheridan Books, 2000).
However, the contemporary concept of privacy was first developed as an independent legal value when Brandeis and Warren identified it as a tort action, defining it as 'the right to be left alone'. See Warren S and Brandeis L, "The Right to Privacy" 4 *Harvard Law Review* (1890), 193–220.

2 Cfr De Hert P and Gutwirth S, "Data Protection in the Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in Gutwirth S et al (eds.) *Reinventing Data Protection?* (Springer, 2009), 3-44; Lynskey O, "Deconstructing Data Protection: The 'Added-Value' of A Right to Data Protection in the EU Legal Order", 63(3) *International and Comparative Law Quarterly* (2014), 569–597.

3 Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31–50.

Consequently, the EU Commission has reviewed the former legal framework for data protection to modernise it vis-à-vis the new upgraded Treaty framework for data protection, as well as the challenges posed by technologies and globalisation. The Commission's proposal updated the principles enshrined in the 1995 Data Protection Directive to guarantee enhanced data protection rights in the future. They included a policy Communication setting out the Commission's objectives and two legislative proposals:

> (1) a proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or GDPR), which sets out a general EU framework for data protection;[4] and
> (2) a proposal for a directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.[5]

The Commission's proposals have gone through lengthy negotiations between the European Parliament and the Council of Ministers for discussion and approval. The final texts were approved by the EU Parliament on 14 April 2016. The GDPR is directly enforceable from 25 May 2018 in all Member States (Art 99 of the GDPR). It is set to lead to a uniform application and enforcement of data protection law across EU jurisdictions. In contrast to a 'Directive', the use of the legal form of a 'Regulation' means that it has direct effect and does not need national implementation. This is designed to eliminate risks of national particularities and diversity of practices, which would frustrate the goal of using that precise EU legal instrument to achieve uniformity. Instead, Directive (EU) 2016/680 provides for the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.[6]

To fully understand the nature, scope and provisions of current European data protection law, it is important to understand its origins and evolution, which occurred at international level. In fact, European data protection law was preceded by the Council of Europe Convention of 28 January 1981 'for the protection of individuals with regard to automatic processing of personal data' ('Treaty 108'). The Council of Europe, whose 46 Member States include the 27 EU Member States, was established in 1949 and is the continent's oldest political organisation, most famous for its activity in the field of human rights. The Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the European Court of Human Rights are both emanations of the Council.

EU data controllers, as well as practitioners and students of data protection laws require an understanding of European and international laws in the field: the GDPR was reactive to pre-

4 COM/2012/011 final.

5 COM/2012/010 final.

6 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, OJ L 119, 4.5.2016, 1–88 and Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, 89–131.

existing European and international advances in the field, and domestic law is increasingly permeated by these external influences. Furthermore, data controllers can be subject to foreign regulation depending upon how they structure their data processing operations.[7]

The Council of Europe Activity in Data Protection

The Statute of the Council of Europe and the Protection of Human Rights

The Statute of the Council of Europe of 5 May 1949 provides the legal foundation for the Council and for all its subsequent activities, including Convention 108. The aim of the Council is described in Art 1 of the Statute:

> *"The aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safe-guarding and realising the ideals and principles which are their common heritage and facilitating their economic and social progress."*

Article 3 of the Statute explains that achievement of the aim is contingent upon commitment to the rule of law and respect for human rights and fundamental freedoms:
'Every member of the Council of Europe must accept the principles of the rule of law and of the enjoyment by all persons within its jurisdiction of human rights and fundamental freedoms, and collaborate sincerely and effectively in the realisation of the aim of the Council as specified in Chapter I.'

The Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)

The ECHR of 4 November 1950 is arguably the most well-known legal instrument of the Council of Europe. Article 8 provides:

> *'1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

The ECHR has been incorporated into the domestic laws of the Member States, which require primary legislation and subordinate legislation to be read and given effect in a way which is compatible with the Convention rights, so far as it is possible to do so, as well as making it unlawful for a public authority to act in a way that is incompatible with a Convention right.

The Genesis of Council of Europe Activity in Data Protection

The spur to Council of Europe activity in the field of data protection was an emerging concern in the mid-late 1960s about the ability of the ECHR to adequately protect personal privacy within the context of increasing computerisation and other advances in technology. The following passage is taken from the explanatory report to Convention 108:

7 See, also, Milanovic M, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", 56(1) *Harvard International Law Journal* (2015), 81.

> *'In 1968, the Parliamentary Assembly of the Council of Europe addressed Recommendation 509[8] to the Committee of Ministers asking it to examine whether the European Human Rights Convention and the domestic law of the Member States offered adequate protection to the right of personal privacy vis-à-vis modern science and technology.*[9]

A study carried out on instruction of the Committee of Ministers in response to that recommendation showed that the present national legislations gave insufficient protection to individual privacy and other rights and interests of individuals with regard to automated data banks.
On the basis of these findings, the Committee of Ministers adopted in 1973 and 1974 two resolutions on data protection. The first, Resolution (73) 22 established principles of data protection for the private sector and the second, Resolution (74) 29 did the same for the public sector.'
The Council's concern about the adequacy of the ECHR was essentially threefold:

- Article 8 was concerned only with interferences with privacy by public authorities, not interferences by private parties;
- Article 8 was concerned with the protection of privacy in a limited sense, such as privacy in correspondence;
- it was a closed Convention that did not permit the participation of non-European and non-Member States.[10]

Thus, the Council of Europe Resolution (73)22 was the first substantial legal instrument specifically concerned with data protection. The explanatory report to the Resolution illuminates further the human rights aspect of data protection, the concerns about the adequacy of the ECHR and the threat to personal privacy consequent upon advances in technology:

> *'1. It is generally recognised that the development of modern science and technology, which enable man to attain an advanced standard of living, brings in its wake certain dangers threatening the rights of individuals.*
>
> *This is the case, for instance, with the utilisation of new techniques for surveillance or observation of persons and for compiling and processing data pertaining to them,*
>
> *2. A survey, conducted in 1968-70 by the Committee of Experts on Human Rights of the Council of Europe, on the legislation of the Member States with regard to human rights and modern scientific and technological developments has shown that the existing law does not provide sufficient protection for the citizen against intrusions on privacy by technical devices. Generally, the existing laws touch upon the protection of privacy only from a limited point of view, such as secrecy of correspondence and telecommunications, inviolability of the domicile etc.*

8 Recommendation 509 of the Parliamentary Assembly contained two recommendations to the Committee of Ministers: (i) to study and report on the question whether, having regard to Article 8 of the Convention on Human Rights, the national legislation in the Member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods; (ii) if the answer to this question is in the negative, to make recommendations for the better protection of the right of privacy.

9 The third recital to the Recommendation expressed the fears of the Parliamentary Assembly: 'Believing that newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights.'

10 The explanatory report to Convention 108 explained 'It does not seem advisable, however, to rely solely on the European Human Rights Convention for data protection, inter alia because it is a "closed" instrument, which does not permit the participation of non-European and non-Member States'. To date no non-European countries have taken advantage of the opportunity to sign Convention 108.

Moreover, the ramifications of the concept of privacy have never been established. It is also doubtful whether the European Convention on Human Rights, of which Article 8 (1) guarantees to everyone "the right to respect for his private and family life, his home and his correspondence", offers satisfactory safeguards against technological intrusions into privacy. The Committee of Experts on Human Rights has noted, for example, that the Convention takes into account only interferences with private life by public authorities, not by private parties.

3. A particular new source of possible intrusion into privacy has been created by the rapid growth and popularisation of computer technology. The purposes which computers are increasingly serving in the public and private sectors are by themselves not basically different from those served by more traditional forms of data storage and processing.

What is setting computers apart from the traditional means of data storage and processing is the extraordinary ease with which they have overcome at a stroke a whole series of problems raised by the management of information: the great volume of data, the techniques for their storage and retrieval, their transmission over large distances, their correct interpretation and, finally, the speed with which all these operations can be performed.

Thus, computers permit the building up in the form of "data banks", of data collections or integrated networks of data collections. These "data banks" are capable of providing instantly and over large distances massive information on individuals. While few would deny the great advantages offered by the application of electronic data processing techniques, there is a growing concern among the public about the possibility of improper use being made of sensitive personal information stored electronically.

It is, for example, much more difficult for an individual to take steps to protect his personal interests vis-à-vis a computerised information system than it is with regard to a traditional data register. Moreover, data concerning him, which are by themselves inoffensive, may be correlated in such a way that their availability becomes a threat to his private interests.'

The Annex to the Resolution contains a list of ten principles applying to personal information stored in electronic data banks in the private sector, as well as the first substantial definitions of 'personal information' and electronic processing. These principles and definitions have remained remarkably consistent since 1973, with Convention 108, the Data Protection Directive and the implementing national laws of the EU Member States adopting very similar formulations:

"The following principles apply to personal information stored in electronic data banks in the private sector.

For the purposes of this resolution, the term "personal information" means information relating to individuals (physical persons), and the term "electronic data bank" means any electronic data processing system which is used to handle personal information and to disseminate such information.

1. The information stored should be accurate and should be kept up to date.
In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

2. The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3. The information should not be obtained by fraudulent or unfair means.

4. Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used.

5. Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

6. As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

7. Every care should be taken to correct inaccurate information and to erase, obsolete information or information obtained in an unlawful way.

8. Precautions should be taken against any abuse or misuse of information.
Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirection of information, whether intentional or not.

9. Access to the information stored should be confined to persons who have a valid reason to know it.

The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

10. Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person."

In turn, the Annex to Resolution (74)29 repeats the definition of personal data used in Resolution (73)22, makes only minor adjustments to the definition of electronic processing and reduces the number of principles from ten to eight whilst giving them greater precision:
'The following principles apply to personal information stored in electronic data banks in the public sector.
For the purposes of this resolution, "personal information" means information relating to individuals (physical persons) and "electronic data bank" means any electronic data processing system, which is used to handle such information.

1. As a general rule the public should be kept regularly informed about the establishment, operation and development of electronic data banks in the public sector.
2. The information stored should be:
a. obtained by lawful and fair means,

b. accurate and kept up to date,
c. appropriate and relevant to the purpose for which it has been stored.
Every care should be taken to correct inaccurate information and to erase inappropriate, irrelevant or obsolete information.

3. Especially when electronic data banks process information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination,

a. their existence must have been provided for by law, or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state;
b. such law, regulation, statement or document must clearly state the purpose of storage and use of such information, as well as the conditions under which it may be communicated either within the public administration or to private persons or bodies;
c. that data stored must be used for purposes other than those which have been defined unless exception is explicitly permitted by law, is granted by a competent authority or the rules for the use of the electronic data bank are amended.

4. Rules should be laid down to specify the time limits beyond which certain categories of information may not be kept or used.

However, exceptions from this principle are acceptable if the use of the information for statistical, scientific or historical purposes requires its conservation for an indefinite duration. In that case, precautions should be taken to ensure that the privacy of the individuals concerned will not be prejudiced.

5. Every individual should have the right to know the information stored about him. Any exception to this principle or limitation to the exercise of this right should be strictly regulated.

6. Precautions should be taken against any abuse or misuse of information. For this reason:
a. everyone concerned with the operation of electronic data processing should be bound by rules of conduct aimed at preventing the misuse of data and in particular by a duty to observe secrecy;
b. electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information and which provide for the detection of misdirection of information, whether intentional or not.

7. Access to information that may not be freely communicated to the public should be confined to the persons whose functions entitle them to take cognisance of it in order to carry out their duties.

8. When information is used for statistical purposes it should be released only in such a way that it is impossible to link information to a particular person.'

Convention 108 and Its Relevance for Data Protection Law

Resolutions (73)22 and (74)29 both required the Council of Europe Member States to take all the steps that they considered necessary to give effect to the principles contained in the Annexes. This left the Member States with considerable room for manoeuvre, leading to divergences in national laws. Indeed, the explanatory report to Convention 108 reveals:

> *'there is a lack of general rules on the storage and use of personal information and in particular, on the question of how individuals can be enabled to exercise control over information relating to themselves which is collected and used by others.'*

Although it was left to the discretion of the Member States by what means they would give effect to these rules, practically all States have decided to do so by legislation. In three Member States, data protection has been incorporated as a fundamental right in the Constitution (Article 35 of the 1976 Constitution of Portugal; Article 18 of the 1978 Constitution of Spain; Article 1 of the 1978 Austrian Fundamental Right of Data Protection). The Parliamentary Assembly of the Council of Europe, taking the latter tendency into account, recommended in its Recommendation 890 (1980) to study the possibility of including in the ECHR a provision on the protection of personal data.

While the procedural rules differed from one country to another, there was a large measure of agreement on the objectives to be satisfied by these rules. All national laws recognised: i). the principle of publicity, i.e. that the existence of automated data files should be publicly known; and ii) the principle of control, i.e. that public supervisory authorities as well as the individuals directly concerned by the information can require that the rights and interests of those individuals are respected by the data users.

In most countries the data protection law had a wide scope and applied to data processing in the public sector as well as the private sector. In some countries, moreover, not only automated files but also certain categories of manual files fell within its area of application. In all countries the legislation covered data relating to natural persons, but in some it also covers data concerning legal persons. Where, for reasons of public interest, certain restrictions or exceptions from the general rules were necessary, these were generally spelled out by the law itself.[11]

In addition to the desire to remedy the perceived inadequacies of the ECHR, the explanatory report to Convention 108 revealed another significant driver to legislation, namely the interest in maintaining transborder data flows:

> *"The question has arisen to what extent national data protection laws afford adequate protection to individuals when data concerning them flow across borders. Computers, in combination with telecommunications, are opening new prospects for data processing on an international scale. They help to overcome several types of barrier to communication between nations: distance, time, language and cost. Distributed processing enables users to disperse an information system or data base over several countries. Networks help users to have access to or link information systems in distant countries. In several sectors (for example banking, travel, credit cards, etc.) such transfrontier data processing applications are already commonplace. In principle, it should make no difference for data users or data subjects whether data processing operations take place in one or in several countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests.*

11 Korff D, "Comparative summary of national laws", *EC Study on Implementation of Data Protection Directive* (Study Contract ETD/2001/B5 3001/A/49), Human Rights Centre, University of Essex (Colchester, 2002).

> *In practice, however, protection of persons grows weaker when the geographic area is widened. Concern has been expressed that data users might seek to avoid data protection controls by moving their operations, in whole or in part, to "data havens", ie countries which have less strict data protection laws, or none at all.*
>
> *In order to counter this risk some countries have built into their domestic law special controls, for example in the form of a licence for export.*
>
> *However, such controls may interfere with the free international flow of information which is a principle of fundamental importance for individuals as well as nations. A formula had to be found to make sure that data protection at the international level does not prejudice this principle."*

Thus, by January 1981, the Council of Europe's actions were motivated by:

- concerns about the adequacy of the ECHR;
- concerns about disparities in national laws;
- a desire to maintain transborder data flows.

The Preamble to Convention 108 reflects this. It affirms the aim of the Council of Europe to achieve greater unity between its members on the respect for the rule of law and human rights; it extens the safeguards for everyone's rights, particularly the right to privacy in an increasing flow across frontiers of personal data undergoing automatic processing; it reaffirms the commitment to freedom of information regardless of frontiers; it recognises the need to reconcile the respect for privacy and the free flow of information between peoples.

These issues were also at the heart of the Data Protection Directive and, later, of the Treaty of the Functioning of the European Union, the Charter of Fundamental Rights of the EU, and the GDPR.

Structure and Content of Convention 108

Convention 108 requires Member States to apply its provisions to public sector and private sector automated processing only, whilst recognising that they may extend their domestic rules to manual files. Its object and purpose, which it calls 'data protection', is contained in Art 1:

> *'The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").'*

The main structure of the Convention early recognised the following:

- **Quality of data** – Article 5 provides that personal data undergoing automated processing shall be: (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in ways incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; and (e) preserved in a form that permits identification of the data subject for no longer than is required for the purposes for which the data are stored.

- **Special categories of data** – Article 6 provides that special category data shall not be processed automatically in the absence of adequate safeguards in domestic law. Special

category data is: (a) personal data revealing racial origins, political opinions or religious or other beliefs; (b) personal data concerning health or sexual life; and (c) personal data relating to criminal convictions.

- **Data security** – Article 7 requires appropriate measures to be taken for the protection of personal data stored in automated data files. This is to guard against: (a) accidental or unauthorised destruction; (b) accidental loss; and (c) unauthorised access, alteration or dissemination.

- **Additional safeguards for data subjects** – Article 8 provides data subjects with a series of personal rights. These enable the data subject to: (a) establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; (b) obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; (c) obtain rectification or erasure of such data if they have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Arts 5 and 6; and (d) a remedy if a request for confirmation or communication, rectification or erasure is not complied with.

- **Exceptions and restrictions** – Article 9 provides the member state with the power to make derogations from the requirements of Arts 5, 6 and 8, where the derogations are necessary to protect state and public interests, or in the interests of the data subject or third parties, together with a power to limit the access rights in Art 8, where the processing is for statistics or scientific research.

- **Sanctions and remedies** – Article 10 requires Member States to provide for appropriate penalties and remedies for violation of domestic laws.

- **Transborder data flows** – Article 12 provides, subject to derogations, that Member States may not prohibit or restrict transborder data flows (transfers across national borders), or make them subject to authorisations on the ground of protection of privacy. Member States may derogate from this rule, except where the recipient country provides 'equivalent protection' to that provided by national legislation.

These principles early reflect the later normative provisions of EU law and its evolutions.

The Continuing Relevance of the Council of Europe, Convention 108+ and Its Relationship with the GDPR

During the early stages of European activity in data protection the EU (then EEC) was willing to allow the Council of Europe to take the lead in the development of policy. As the explanatory report to Convention 108 explains:

> *"The Commission of the European Communities, which carried out studies concerning harmonisation of national legislation within the Community in relation to transborder data flows and possible distortions of competition, as well as problems of data security, kept in close touch with the Council of Europe. The Commission decided to await the outcome of the work on this convention before deciding on its own action in the field of data protection. The European Parliament also expressed*

> *a deep interest in data protection. At its May 1979 session it adopted a resolution on the protection of the rights of the individual in the face of technical developments in data processing which it forwarded to the Committee of Ministers of the Council of Europe."*

Six months after Convention 108 was opened for signature the EU (then EEC) Commission issued a Recommendation,[12] that those Member States that had not already done so to sign Convention 108 for the protection of individuals with regard to automatic processing of personal data, and to ratify it before the end of 1982. The Commission reserved the right to propose that the Council adopt an instrument on the basis of the EU (then EEC) Treaty' in the event that all the Member States did not within a reasonable time sign and ratify the convention. The Commission eventually exercised this right, with its proposal for a Data Protection Directive in 1990.

Despite an expansive EU, the emergence of the Data Protection Directive and the unwillingness of non-Council of Europe States to sign up and ratify Convention 108, the Council of Europe and Convention 108 have continued to enjoy great influence.[13]

Factors in the Council of Europe's favour include the size of its membership (46 Member States), its function in the EU enlargement process (all EU Member States have first been Council of Europe Member States), its age and history (generally and in respect of data protection), its special focus on human rights and fundamental freedoms, its prestige work in related areas (e.g. the Cybercrime Convention), its ownership of the world famous European Convention on Human Rights, and continuing uncertainty over the extent of EU competence in the area of human rights. The Council of Europe maintains prominence through the issue of Recommendations. These Recommendations approach data protection from a sectoral perspective, drawing attention to substantial matters of concern. These Recommendations carry influence within the EU. For example, Council of Europe Recommendation[14] on the protection of personal data collected and processed for insurance purposes was supported by the EU Commission.[15]

A process of modernisation of Convention 108 has been launched in 2011, which marked the beginning of a public consultation organised in this context.

On 18 May 2018, one week before the GDPR came into force, the modernisation of Convention 108 was completed by the Council of Europe, with the parties to the existing Treaty agreeing to a Protocol amending it ('Convention 108+').

The need for global data protection standards and the adaptation to the GDPR prompted the adoption of Convention 108+, which can be signed and ratified by any country around the world. Given the increasing data flows, having different degrees of data protection in different regions would represent a threat to those countries and regions that are advanced in their legislations (e.g. the EU). Harmonisation among countries around the world is also key to ensuring that enforcement is equally strong everywhere, and companies do not engage in forum shopping

12 Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (81/679/EEC).

13 See, also, de Hert P and Papakostantinou V, "The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition", 30(6) *Computer Law & Security Review* (2014), 633-642.

14 Recommendation Rec(2002)9 of the Committee of Ministers to Member States on the protection of personal data collected and processed for insurance purposes.

15 Recommendation for a Council Decision on the vote to be taken by Member States within the competent bodies of the Council of Europe, on behalf of the European Community, in favour of adopting the draft Recommendation on the protection of personal data collected and processed for insurance purposes, and of authorising the publication of its Explanatory Memorandum (SEC/2002/0280 final), 18 March 2002.

processing data in jurisdictions with lower levels of protection.

Any individual is covered by its protection, independently of their nationality, as long as they are within the jurisdiction of one of the parties who have ratified the Convention.

All EU Member States ratified Convention 108+. At present, 55 countries are parties including all Member States of the Council of Europe (46 countries), Uruguay (the first non-CoE country to accede), Argentina, Mexico, Cape Verde, Burkina Faso, Morocco, Mauritius, Senegal, and Tunisia. The EU as a supranational body is also a party to the Convention 108+.

The EU sees the protocol as a way of encouraging third countries to adopt the basic tenets of the GDPR. In fact, accession to Convention 108+ carries a positive effect on applications for 'adequacy' assessments to the EU under the GDPR. In legal terms, what Recital 105 of the GDPR provides is that the European Commission should take account of obligations arising from the third country's participation in multilateral or regional systems. In particular, the third country's accession to Convention 108+ should be taken into account. Nonetheless, the extent to which compliance with Convention 108+ will be sufficient for EU adequacy is still uncertain.

Conclusion

The Council of Europe and EU law share common origins and principles. EU law now aims to become the global data protection standard that, by means of its adequacy criterion, is exporting to third countries.

From its part, the Council of Europe Convention constituted a binding text that came to be addressed predominantly to States that are also EU members committing to data protection law. For third countries, the option for ratification signals an attempt for the Council of Europe to contribute to the achievement of a global standard. At international level, it represents the only mandatory text regulating the processing of law enforcement agencies. All personal data processing is to be governed by its provisions, including therefore both public and private sector as well as that of law enforcement agencies.[16]

Its interconnectedness with the ECHR and to the European Court of Human Rights provides an individual right to data protection as a spin-off of the human right to privacy.[17]

However, the relationship between the right to privacy and the right to data protection in the ECHR remains unclear. Instead, EU law has clearly distinguished the right to data protection from the right to privacy, giving them an independent, standalone status in the text of its Treaty. In this way, data protection has evolved in autonomous principles in the GDPR rather than remaining guidelines derived from the general right to privacy.

Through this process, nowadays the EU actively promotes its data protection legislation via its adequacy system.

Nonetheless, in a fragmented international environment and the absence of a globally accepted data protection legislation standard, it is important to have a formal set of rules open to non-members of the EU such as that of now Convention 108+. Its adherence is increasingly becoming a positive element for the EU adequacy requirements, thus showing how international laws have not only shaped EU law but continue to have a prominent autonomous relevance.

16 de Hert and Papakostantinou, cit. supra note 13.

17 de Hert P and Gutwirth S, "Data Protection in the Case Law of Strasbourg and Luxembrourg: Constitualisation in Action," in Gutwirth et al (eds.) *Reinventing Data Protection?*, (Springer, 2009), 3–44.

Privacy and Data Protection

A Thought on Child's Best Interest in Data Protection

Dr. Boshe Patricia

[t]he confidence and the innocence . . . of children whose world has ever been practically a safe one.... is the one that meets the greatest number of social appearances.
Maeve Pearson: The Paradox of Children's Privacy

Introduction

Until recent, the protection of children's[1] personal data and privacy had not summoned the deserving attention. The word "child" or "minor" was missing in laws protecting personal data. It was neither in the first world's comprehensive data protection law of 1978[2] nor the first and the only international legally binding data protection instrument, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of 1981. The same thing with the first European Union regional framework for data protection (Directive 95/46/EC). A child was neither mentioned nor any special attention in protecting their privacy and personal data was indicated.

The EU changed this stance in 2016, when the General Data Protection Regulation (GDPR) replaced the Directive 95/46/EC. The GDPR introduced Article 8, regulating the processing of personal data of a child. However, this provision is limited to the processing of child's data "in relation to the offer of information society services directly to a child".[3] In which case, the processing of child's data requires a consent of a parent or legal guardian. As further stipulated in Recital 38, the rationale for Article 8 is the fact that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data." Accordingly, the consent for the processing of a child's data is the right given exclusively to the "holder of parental responsibility". The latter has the right to consent, deny and withdraw consent for the processing of child's data in the said context.

Unfortunately, the GDPR is not explicitly on the conditions for the processing of children's data when the processing is based on other legal bases. It is not clear whether, for example, when the processing of child's data is necessary for compliance with a certain legal obligation (to which the controller is a party), would a parent/ legal guardian still have a role to play or a say over such processing activities? Would a parent/ legal guardian be able to request access, deletion, rectification of the child's data involved in the said processing activities?

Another challenge associated with consent as the 'only' identified basis for the processing of children's data is the fact that, a parent / legal guardian is (maybe) also the primary data controller of the child's data. In fact, parents / legal guardians happen to be the 'best' processors of (their) children's data – including sensitive data, audio and image data – on online platforms. Such practices are considered as 'normal' part of parenting, leading to a connotation 'Sharenting', i.e. sharing is parenting. It begs the question, how and who determines the child's best interest in a situation when a parent / guardian processes child's personal data for their own amusement, or as part of their parenting – in absence of child's involvement and in disregard of what might be the child's wish and best interest?

1 A definition of a child, in the context of processing their personal data, may vary between jurisdictions. Some jurisdiction would define a child as a person who has not attained the age of sixteen years, and others would refer to the definition of a child as provided under respective child laws of the specific country – which most often is eighteen years.

2 Datalagen (Data Act (1973:289)).

3 See Article 8 of the GDPR.

As the debate on child privacy, data protection and safety online is taking precedence, this chapter intends to assess different data protection frameworks in the attempt and approaches to protecting child's data and privacy rights. In doing so, gaps and best practices are identified and recommendations for improving children's data and privacy protection are drawn. This chapter is written in cognizance of the ever-growing presence of children online[4] and the increased processing of children data both on and offline[5]. Also, is the fact that, children, unlike adults, are more vulnerable and may lack the capacity to assess and appreciate the dangers that comes with their (data) presence online[6] and in the use of automated processing machines. The essence of the chapter is therefore, to provide recommendations for legislative consideration to strengthen the protection of children's personal data and privacy.

Internet of Things and the Protection of Children's Personal Data

A report written for the UNICEF acknowledges the risks children face in the processing of their data beyond an offline context. The report noted, although access to the internet allows the young generation to experiences and opens up new opportunities for children, their development and how they can express themselves and their civic engagement[7], their presence there allows for the collection of their personal data which exposes them to "fresh challenges that deserve special attention, especially those surrounding privacy… [but have an effect] on other rights such as freedom of expression, access to information and public participation."[8]

Another downside of technology is the ability to process huge amounts of personal data using data mining techniques. This can adversely impact on the privacy of children who have presence on online platforms. Moreso, since children may lack proper knowledge on the risks of processing activities undertaken online. The latter range from online surveillance techniques, profiling and behavior assessment etc.

In 2015, a Global Privacy Enforcement Network (GPEN) conducted a survey to ascertain the nature of risks against risk mitigations strategies in place to minimize such risks to children's privacy online and misuse of children personal data. The survey found out that, "two thirds of the 1,494 websites and apps surveyed had no protective controls to enable children (or their parents) to limit the disclosure of personal data".[9] Another survey conducted a year later, in 2016, verified that about 59 per cent of the IoT devices surveyed failed to provide sufficient information on how they collect, use and disclose users' personal information[10]. In the same year, the World Health Organization (WHO) reported that online food advertisements that are aimed at children employed profiling techniques to target children. A practice that parents were unaware of.[11] WHO

4 Sonia Livingstone, John Carr and Jasmina Byrne, "One in Three: Internet Governance and Children's Rights"'(Global Commission on Internet Governance Paper Series No. 22. 2015), no22_2.pdf (cigionline.org) accessed on 15.09.2023.

5 Children not only enjoy exciting opportunities of playing, creating, learning, self-expressing, experimenting with relationships and identities, but are also disclosing increasing amounts of their personal data. Cf. Milda Macenaite and Eleni Kosta, "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?", Information & Communications Technology Law 22, no 2 (2017)146.

6 Macenaite and Kosta, "Consent for Processing", p. 147.

7 Mario Viola de Azevedo Cunha, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy", (Innocenti Discussion Paper 2017-03), UNICEF Office of Research – Innocenti, p. 6.

8 Ibid., 3.

9 Privacy Commissioner New Zealand, "Global Privacy Enforcement Network (GPEN) Privacy Sweep 2015: Concerns over Children's Apps and Websites", < International Report Draft (privacy.org.nz) >, accessed on 15.09.2023.

10 Information Commissioner UK, "Global Privacy Enforcement Network (GPEN) Privacy Sweep 2016: Internet of Things", <irq0648379-attachment.pdf (ico.org.uk)> accessed on 15.09.2023.

11 WHO, "Tackling Food Marketing to Children in a Digital World: Transdisciplinary Perspectives", (WHO Regional Office for Europe, Copenhagen, 2016): 4, <Tackling food marketing to children in a digital world: trans-disciplinary perspectives - en (who.int) >, accessed on 15.09.2023.

findings align with results from other researches, that both children and parents are neither unaware of data processing activities deployed by online service providers, nor risks exposed to children from such processing activities.[12] According to the previously mentioned UNICEF report, they also lack "skills and tools necessary to keep track of their data and exercise their rights as data subjects."[13]

This ignorance is (mis)used by service providers (including governments institutions and private organisations) to deploy data mining tools "to track, store, and analyse children's actions with a level of detail previously unattainable"[14] Since spending time online is the main activity children do, it makes them a crucial consumer segment. According to Doneda and Rossini, children influence consumer decision by families and hence forms an important social segment market. It follows therefore, tracking children's online activities and behaviors, profiling them and target advertisement, forms an effective commercial strategy. One that determines market share (at least in an online context). As a result, their lives are explored, exploited, analysed and mimicked to influence their online experiences for, among other things, commercial gain.[15]

Personal data, freely given by children online are used for purpose 'unknown' to children and parents. This not only poses privacy related risks, but also real-time physical and mental danger to children. An example of such dangers is the increased rate of children and adolescent suicide[16] and mental health issues[17]. Online service providers are able to deploy and use technology with an ability to identify and target vulnerabilities and use it 'anyhow'. An attorney from a US based Social Media Victim Law Centre, Ms. Laura Marquez-Garrett noted that, it is hard for a parent to notice the dark side of online Apps such as TikTok as "you could have a child and parent in the same room together watching TikTok on their phones and they'd be seeing an entirely different product"[18]

Otherwise, algorithm (drove by data) through automated decisions can use existing (online) data, whose use could lead to discrimination – either based on (child's) ethnicity and/ or religious status, color, gender or nationality. This has an impact on children's future career prospects, both socially and professionally. It could even increase their exposure to state surveillance, as argued in the UNICEF report, "should they appear to correspond to a group that is more likely to exhibit criminal behaviour in future."[19]

12 Cf. Sonia Livingstone, John Carr and Jasmina Byrne, "One in Three"; Lina Jasmontaite and Paul De Hert, "The EU, Children under 13 years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet", International Data Privacy Law 5, no. 1, (2015), 20.

13 Mario Viola de Azevedo Cunha, "Child Privacy," 7.

14 Duncan Brown and Norma Pecora, "Online Data Privacy as a Children's Media Right: Toward Global Policy Principles", Journal of Children and Media 8, no. 2, (2014), 201.

15 According to UNICEF report (Mario Viola de Azevedo Cunha, "Child Privacy," 10), the main processors of children data include corporations whose main purpose is to collect, analyze and sale of children's browsing data, and government surveillance. Cf. Valerie Steeves, "It's Not Child's Play: The Online Invasion of Children's Privacy', University of Ottawa Law & Technology Journal 3, no. 1, (July 2007), 169.; Federica Casarosa, "Protection of Minors Online: Available Regulatory Approaches", Journal of Internet Law 9, (March 2011), 25.

16 An example is suicide incidences triggered by TikTok's use of algorithm with suicide encouraging content and that led to several suicide and severe physical harm. Cf. Kyra Colah, "7 dangerous TikTok challenges for kids that parents must know about: 'Extreme and risky'," March 19, 2023 <https://www.fox10phoenix.com/news/dangerous-tiktok-challenges-list-kids-parents-march-2023> accessed on 20.09.2023.

17 Resulting from cyberbullying.

18 Olivia Carville, "TikTok's Algorithm Keeps Pushing Suicide to Vulnerable Kids," April 20, 2023 <https://www.bloomberg.com/news/features/2023-04-20/tiktok-effects-on-mental-health-in-focus-after-teen-suicide?embedded-checkout=true> accessed on 20.09.2023.

19 Mario Viola de Azevedo Cunha, "Child Privacy," 10.

There are many such instances and reports on harm resulting from using online platforms. However, this discussion is beyond the purview of the present chapter. Nevertheless, a short narration of data practices and potential harms was necessary to illustrate the depth of the problem and identify regulatory silos.

Sharenting and the Protection of Children's Data

Children are not the only segment 'freely' feeding governments and corporations with their data. Parents share a great amount of children data with or without their children's knowledge and 'approval'. It is now a "commonplace for parents to share information about their children online".[20] The so called 'sharenting'. Often, children are unaware of sharenting and existence of their data (including images and videos) and therefore, unable protest or object to the sharenting.[21] Stacey Steinberg is of the opinion that parents' ought to ask for their children approval before they could consent to any processing activity, or post any of the children's data online.

Beyond sharenting, solely relying on parental control (consent) "opposes the idea of children's participation in the decision-making process that concerns them – an idea that is anchored in the UN Convention of the Rights of Children"[22] Parental consent may also subject a child to an invasion of their privacy. For a parent to consent to processing activities, (such the use of social media and gaming platforms) they must access, see and decide on whether or not to give consent to activities a child wishes to participate in. Children may not be ready to share all their online experiences with their parents. Parental access in this regard goes along with the exercise of other rights such as the right request removal of content, rectification and block processing activities. According to Wonsun Shin and Hyunjin Kang, this approach to protecting children's data "reduces children's autonomy and freedom online".[23] They are of the view that, "[c]hildren have the right to express their views on all matters that affect them, and can express their views independently from their parents on matters that affect them, even when such opinions defer from those of their parents."[24] However, considering maturity level, to exercise their autonomy, children may, as recommended by the Committee on the Rights of the Child[25], require guidance on their rights and how to protect themselves, even within the family.

The virtual world increasingly engulfs the physical world. As a place for people to exercise their civic rights, build their images, and interact with others. It therefore, forms part of an individual identity. The safety of children who are inevitably a large part of the virtual world (forming 1/3 of all internet users)[26], which transcend borders, depends on government efforts to develop suitable policies and laws to regulate the safety of children online – and beyond.

Despite the dangers posed during processing children's data online, a call to ban 'harmful' online platform is discouraged by scientists. A blanket ban is considered as not being effective. One of the scientists, Dr. Rutlege says, "[b]ans are like holding beach balls under water, you can ban one platform, but another platform will always pop-up".[27]

20 Carly Nyst, "Privacy, Protection of Personal Information and Reputation Rights," Children's Rights and Business in a Digital World Discussion Paper Series, (United Nations Children's Fund, March 2017).

21 See Mario Viola de Azevedo Cunha, "Child Privacy," 10 quoting Stacey Steinberg, "Sharenting: Children's Privacy in the Age of Social Media," Emory Law Journal 66, (2017) 839.

22 Lina Jasmontaite and Paul De Hert, "The EU, Children under 13 years".

23 Wonsun Shin and Hyunjin Kang, "Adolescents' Privacy Concerns and Information Disclosure Online: The Role of Parents and the Internet," Computers in Human Behavior 54, (January 2016) 114 quoted in Mario Viola de Azevedo Cunha, "Child Privacy,"15.

24 Wonsun Shin and Hyunjin Kang, "Adolescents' Privacy" in Mario Viola de Azevedo Cunha, "Child Privacy," 15.

25 United Nations, Committee on the Rights of the Child, "General Comment No. 20 (2016) on the Implementation of the Rights of the Child during Adolescence," (CRC/C/GC/20, United Nations, 6 December 2016).

26 (Livingstone, Carr and Byrne, 2016),

27 Olivia Carville, "TikTok's Algorithm".

The idea of relying solely on parental intervention "opposes the idea of children's participation in the decision-making process that concerns them – an idea that is anchored in the UN Convention of the Rights of Children" (Jasmontaite and De Hert, 2015). To consent to the processing of their children's personal data, parents must intrude their children's private online spaces (e.g. gaming accounts, social network accounts). As a result, children's access to information and potential to express themselves become both limited and dependent on their parents. Relying mainly on parental consent to protect children's privacy thus reduces children's autonomy and freedom online (Shin and Kang, 2016).

The Essence of Data Protection

In General

Protection of personal data is tandem to the right to self-determination and assertion of individual identity. This is why one of the main pillars in data protection is the involvement of the data subject. This is done by allowing data subjects access to their data to enable them have 'control' on the type of data and nature of processing activities involved in their data. The right to access personal data allows an individual to confirm whether their data is being processed and if so, for what purpose. On confirmation, an individual can further confirm correctness of their data (for the intended purposes) and may request for the correction / rectification, updating of their information, or even request deletion of all or certain data.

A person has the right to decide how he is (re)presented or perceived, through the processing of his personal data. A person may as well decide to 'disappear' from the public through the right to be forgotten. On the other hand, data protection regimes provides for a framework to safeguard personal data (against possible data leakage and the misuse) and on the other hand, gives data subjects the ability to determine the extent and nature of data processed for specific purposes – or not at all.

In Relation to a Child

Research shows that children, as young as 11 face misuse of personal data and are unable to find help or proper reporting tools, including navigating privacy tools to protect themselves.[28] Major concerns include the possibility of misuse of their personal data, damage to their reputation. This could, for example happen as a result of hacking their social media and other online accounts, and use of online scrapped data to create fake profiles and impersonation[29] Yet, there is lack of 'child friendly' rules to protect children. Data protection laws tend to "conflat[e] adults and children in one single group of data subjects."[30]

In addition to this, children's specific rules are in congruity across jurisdictions. No one can single out one global best practice for protecting children's personal data, as the case with the protection of adults' personal data, i.e the GDPR.[31] The good news is that, states and authorities

28 Milda Macenaite and Eleni Kosta, "Consent for Processing", p. 150.

29 Giovanna Mascheroni and Kjartan Ólafsson, Net Children Go Mobile: Risks and Opportunities (2nd edn Educatt, Milan 2014).

30 Milda Macenaite and Eleni Kosta, "Consent for Processing", p.148.

31 The GDPR is argued to be a "golden standard" (as claimed by Viviane Reding during the drafting of the GDPR). Also, trends in assimilate the GDPR framework across the globe would speak of its 'acceptable global standards'. Although many scholars reject this assertion claiming that third countries adopting GDPR "have little to no option but to assimilate the EU data protection framework to sustain cross border data flows (Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (Oxford University Press 2019).) and maintain international trade (Lee A. Bygrave, Data Privacy Laws: An International Perspective (Oxford University Press 2014). Kuner further believes that, since EU standards must remain applicable for data flows to take place makes the EU framework highly competitive against other privacy and data protection frameworks such as the US and Asia.

are increasingly appreciating this gap and are making attempts to come up with solutions thereof. For example, concerns over the misuse of children personal data prompted some DPAs in Europe to conduct a survey which revealed massive collection and disclosure of children personal data and absence of child-tailored privacy policies.[32]This led to the French DPA - *Commission Nationale de l'Informatique et des Libertés* (CNIL) to issue several guidelines to parents and to service providers to remind them of their obligations towards child protection. On the part of service providers (controllers), CNIL reminded them of their obligations to attain parental consent before processing of children personal data[33], and for parents, CNIL of their duty to exercise rights such as 'access' and 'rectification' as one way of safeguarding children's data[34]. The Guideline for parents clarifies children's rights including the right to be forgotten (as provided under Article 40 of the Data Protection Act). According to the Guideline, this right can be exercised by a child him/herself. In making reference to the GDPR, its Recital 65 explains the right of an adult to rectify their personal data or the right be forgotten. According to this Recital, this right also applies to data (and consent) given by such adults when they were still children. At the time when they were "not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet."

Based on this Recital, an adult data subject should be able to exercise the said rights notwithstanding the fact that he or she is no longer a child. It is not expressly stated whether or not this right is available to a child who is not yet an adult and who came to a realization of the mistake or risks involved in the processing of their data and wish to withdraw the consent or exercise their right to be forgotten. It is similarly not clear, as to the role of a parent in such situation where a child consented (in situation beyond those provided under Article 8 of the GDPR) to the processing of the data and no longer wish their data to be processed for the initial specified purposes.

Still, protection of children's personal data is neither straight forward nor sufficiently provided under laws. Jelena Gligorijević attribute the difficulty to unclear rules on parental control in, and consent for the processing of children's personal data. The most important question she asks is how is the role of a parent in the protection of child's personal data "incorporated into laws seeking to protect children's informational privacy?"[35] Her research of courts' jurisprudence in the protection of children personal data indicated that the courts have cemented on parental consent as the basis for the processing of children's personal data. Eventually this led to the creation of a "doctrine that prioritizes parental control and consent, above the harm of intrusion to the child. [As a result, it] risks laying a legal terrain that does not accommodate the protection and vindication of children's informational privacy rights when they conflict with the wishes of, or are not actively protected by, that child's parents."[36] This goes back to the rules for the protection of children personal data within specific legislation. Basically, the courts cannot be blamed as their task is to interpret the rules. And unless a mischief interpretation is invoked, courts would most often give legal provision their literal meaning. In this case, parents have the outmost right and control over personal data of their children.

32 GPEN,'2015 GPEN Sweep–Children's Privacy', 2015 <International Report Draft (privacy.org.nz)> accessed 14.09.2023.
This Sweep research was conducted by 29 DPAs from across regions, and it surveyed around 1494 websites and apps directed towards children.

33 CNIL, "Vie Privée des Enfants : une Protection Insuffisante sur les Sites Internet," <Children's privacy: insufficient protection on websites | CNIL> accessed 14.09.2023.

34 CNIL, "Accompagnez Votre Enfant pour un Usage d'Internet plus sûr," <Accompagnez votre enfant pour un usage d'internet plus sûr | CNIL> accessed 14.09.2023.

35 Jelena Gligorijević, Children's Privacy: The Role of Parental Control and Consent, ANU College of Law Research Paper No 20., p. 1.

36 Ibid.

Of course, consent is just one of the six legal bases for the processing of personal data. However, quite often, when children's data rights are involved, the first 'thought' is legal guardian's consent (or non-thereof). Beyond parental 'control' over the protection of children personal data, is there a better approach to protection of children's data? Could or should laws provide for a better framework that allows for an oversight and intervention over parental control and power in the processing of children's personal data? To what extent should it depend upon parental control and consent?

A look at different approaches to the protection of children's personal data provides an overview and a possible alternative to (better) protect children personal data. The following discussion sheds a light over different legal approaches.

Comparative Overview on Legal Frameworks for the Protection of the Children's Personal Data

Legal Basis for Processing of Children's Personal Data

Consent

GDPR ties the processing of child's personal data to a legal guardian's consent. Moreover, this consent is only stated in the context of service provision by information society to a child. Accordingly, a legal guardian has the power to grant, refuse or withdraw[37] the consent for the processing of child's personal data within that context[38]. This is similar to the legal framework established for the protection of children privacy online under the US Children's Online Privacy Protection Act (COPPA). Different from the GDPR, COPPA is solely dedicated to the protection of children's data and provides for a detailed framework in that effect. The only limitation in both frameworks is their confinement to online context.

In other countries such as Egypt[39], and Kenya[40], legal guardian's consent is provided in general terms. It is not explicitly limited to service provision by information society. Moreover, the two countries, categorises children's personal data as sensitive personal data. This means, like all other sensitive personal data, its processing is prohibited and can only be allowed on specific / exceptional circumstances, and in addition to a written consent of the legal guardian.

In an online context, in Kenya, the law obligates service providers to put in place appropriate mechanisms for age verification, and for consent before the processing of a child's data can take place.[41] Similar provision is seen under Article 14 (5) of the Brazilian General Data Protection Law (GDPL), where a controller is expected to use all reasonable efforts to verify parental / legal guardian's consent – in consideration of available technologies. In India, the law is silent on the age verification requirement but prohibits the tracking or behavioural monitoring of children or targeted advertising directed at children.[42] Egypt has no such provision. However, it has rules in the context where a child participates in social or recreational activities. The law has strict rules of data minimization. It requires that data controllers to collect "only necessary information required for a child to participate on such activity and nothing more.[43]The same requirement is

37 Article 8 GDPR.

38 Recital 38, to the GDPR gives the rationale to Article 8 with respect to consent for the processing of child's personal data that, "[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."

39 Article 1 and 12 of the Data Protection Law of 2020.

40 Section 2 of Kenya Data Protection Act.

41 Section 33 (2) of Kenya Data Protection Act.

42 Section 9(3) of the Digital and Personal Data Protection Act, No. 22 of 2023.

43 Article 12 of the Data Protection Law.

found under Article 14 (4) of the Brazilian GDPL and §6501 (b) (1) (C) US Children's Online Privacy Protection Act (COPPA). The latter adds an additional prohibition. It prohibits the "offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity". COPPA also requires website operators and online service providers "to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[44]

Of the above discussed legal frameworks, it is only in COPPA where a service provider (data controller) can shut down/shut out a child from accessing services if a parent refuses to give consent. The position on other laws is not clear, whether withdrawal of consent equate complete termination of services to a child and any future processing activities. Under the COPPA, once a parent withdraws the consent for processing, it also bars any future online collection of that child's data as well as any form of processing of its data.[45]

Other Legal Bases

Majority of processing activities take place on other bases, i.e. other than the consent of the data subject. In most data protection laws, consent is just one of the six legal bases for the processing of personal data. The other bases include, whenever the processing is necessary, i. to satisfy a contract to which the data subject is a party, ii. to comply with a legal obligation, iii. to protect vital interest of the data subject (or save life of another person), iv. to perform a task in the public interest or to carry out some official function, or v. when there is a legitimate interest to process that data. For the latter legal basis, fundamental rights and freedoms of the data subject must take precedence over whatever legitimate interests.

The above discussed legal framework have not for the other bases in relation to the processing of a child's personal data. In this case, South Africa has such framework. The Protection of Personal Information Act (POPIA) explicitly included the other five legal bases for the processing of personal data if such data is of a child. Section 4 of the POPIA provides for general conditions for the lawful processing of personal data. Furthermore, POPIA creates a 'mini-legal framework' for the processing of children's data.[46] The mini-framework elaborates on lawful processing of a children's personal data – beyond parental / guardian's consent. At the first instance, Section 34 (within this mini-framework) as well as Section 4(3) set a general prohibition on the processing of children's personal data – in general.

One must apply to the DPA (Information Regulator), in case there is a need to process personal data of a child. In such a case, data controller must satisfy two things; first, the processing is in the public interest, and second, appropriate safeguard to protect child's data is in place. Furthermore, before the DPA permit the processing of children's data, a notice in the *Gazette* is published to that effect.[47]

DPA's authorization to process children's data may be also accompanied with additional conditions. The conditions are centred mainly on transparency of processing but also supports other rights such as the right to access, and object processing involved on children's personal data. Other conditions may obligate the data processor to give notice of the quantity of children's data he maintains, and nature of processing activities involved.[48]

44 Subsection (b) (1) (C) of the Child Online Privacy Protection Act.
45 Subsection (b) (3) of the Child Online Privacy Protection Act
46 Part C of POPIA on the Processing of Personal Information of a Child.
47 Section 35 of POPIA.
48 Section 35 (3)(a)(b) of POPIA.

The mini-framework set a condition prohibiting data controllers from encouraging or persuading a child from sharing information beyond what is necessary for the intended purpose.[49] Data controllers are also obligated to establish and maintain a "reasonable procedures to protect the integrity and confidentiality of personal information collected from children."[50]

There are also exemptions where children personal data can be processed in disregard of the above conditions. These are somehow similar to exemption in the processing of adults' personal data, i.e. for law enforcement purposes, or to comply with public international law, or if obtaining consent appears to be impossible and/or would involve disproportionate efforts, or for historical, research and statistical purposes involving public interest, or if personal data of a child was made public by a child with a consent of a parent. In any case, except for the latter, the data controller must put sufficient measure to ensure child's privacy is not adversely interfered with.[51]

Although other countries discussed in this chapter lack such a framework (as South Africa), their laws contain provisions that equate one or more of the other legal bases. In Brazil, for example, the processing of child's and adolescent's personal data is legal if the processing is necessary to contact the parents or the legal representative, and as long as the data are used one single time and not stored. This could fit within the legal basis ii or iii or v above – depending on the context and reasons for contacting parents/legal guardians. Another basis is when data is collected for [child's] protection, and as long as the data is not passed on to third parties without consent of a parent or legal guardian.[52] This would parallel legal basis iii above, i.e. the processing of personal data is necessary to protect vital interests of the data subject. Kenya has a similar approach when it comes to protecting child's interests. Accordingly, it is legal to process personal data of a child if the "data controller or data processor does so in the provision of counselling or child protection services to a child".[53] Also falling within the legal basis iii above, i.e. necessity 'to protect vital interest of a data subject'.

In the US COPPA consent is not required when online processing of a child's data is / was obtained from a child and "is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator."[54] In case there is a need to re-contact a child, COPPA obligates the data controller to use reasonable efforts to notify a parent and inform them of purposes of processing. In which case a parent has the right to object the processing and even request for deletion of such information. However, data controller may as well continue further processing of the child's data without giving notice to a parent. In such an instance, he must ensure the processing are "appropriate" and have considered at least two things; one, the benefit the child has in accessing online information and services, and two the controller has mitigated "risks to security and privacy of the child".[55]

Other instances are where the essence of processing of child's data (name and online contact) is to obtain parental consent, or in order and is "necessary to protect the safety of a child participant on the site." In the latter, the purpose for the processing should be for that purpose only and never to be used to either contact the child or displayed on the site.[56] This is also the case when the processing of child's data is necessary for law enforcement purpose (including legal defense

49 Section 35 (3)(d) of POPIA.
50 Section 35 (3)(e) of POPIA.
51 Section 35 (1)(a-e) of POPIA.
52 Article 14 (3) of the Brazilian General Data Protection Law of 2019.
53 Section 33 (4) Kenya Data Protection Act.
54 15 U.S. Code § 6502 Subsection (b) (2) (A).
55 15 U.S. Code § 6502 Subsection (b) (2)(C)(ii).
56 15 U.S. Code § 6502 Subsection (b) (2)(D)(i-iii).

against controllers' liability) or in implementing security measure to protect personal data and privacy of users' online by the data controller.[57]

In China, parental /guardian's consent is required before processing personal data of a child.[58] The law does not provide for any other requirement or conditions, instead, it shifts the burden to data processors to develop special rules for the processing of children personal data.

Child's Best Interest

There are other countries that have gone beyond the traditional legal bases for the processing of personal data, in order to protect a child. For example, Kenya and Brazil emphasizes on child's best interest. This is in addition to the above-mentioned rules. Data controllers are obligated to ensure, beyond legal basis for the processing of children's personal data, that child's best interest is given primary consideration before any processing activity commences. Section 33 (1) (b) of the Kenya Data Protection Act (KDPA) states;

> *"33. (1) Every data controller or data processor shall not process personal data relating to a child unless — (a) consent is given by the child's parent or guardian; and (b) the processing is in such a manner that protects and advances the rights and best interests of the child."*

In Brazil, GDPL goes a step further by creating a dedicated 'mini framework' for the processing of child's data.[59] Accordingly Article 14 regulates not only the processing of children's data, but also that of adolescents. This provision requires that processing of children and adolescent personal data must be done in their best interest. The law urges that, in determining what best interest entails, reference should be made to what other laws prescribe as the best interest.[60]

Tunisia's and Algeria's, data protection laws also consider the best interest of a child. However, the approach in the two countries is different from that of Kenya and Brazil. In Algeria and Tunisia, a family court judge has the power to override legal guardian's consenting power to protect child's best interest.[61] In this case, a judge may intervene when a parent gives or withheld the consent if he is of the opinion that child's best interest would be affected by parent's / legal guardian's decision to either give or withheld consent to the processing of child's personal data.

Other Actors in the Protection of Children Personal Data

Data Controllers and Data Protection Authorities

Other than legal guardians, data controllers and Data Protection Authorities (DPAs) have a role in the protection of children's personal data. Article 12 of the GDPR requires a data controller – in general – to take appropriate measures to protect personal data. And in specific, to design appropriate measures when [the protection of] a child's data is involved. In this case, the controller should provide relevant processing information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."[62]

57 15 U.S. Code § 6502 Subsection (b) (2)(E)(i-iv).

58 Article 31.

59 Section III of the Brazilian General Data Protection Law of 2019.

60 Article 14 of the Brazilian General Data Protection Law of 2019.

61 Article 8 of the Algeria Data Protection Law (Loi n° 18-07 du 25 Ramadhan 1439 Correspondant au 10 Juin 2018 Relative à la Protection des Personnes Physiques dans le Traitement des Données à Caractère Personnel.), and Article 17 of the Tunisia Data Protection Law (Loi Organique n° 2004-63 du 27 Juillet 2004, Portant sur la Protection des Données à Caractère Personnel).

62 Article 12 GDPR.

In Brazil, the GDPL elaborates further on the above requirement. Article 14 (6) of the GDPL obligate data controllers and processors to not only provide such information in a simple, clear and accessible manner, but to take also into account the physical-motor, perceptive, sensorial, intellectual and mental characteristics of the user, using audiovisual resources when appropriate, in order to provide the necessary information to parents or the legal representative and that is appropriate for the children's understanding.

In addition, the GDPL also requires controllers processing children's and adolescent's data to explain the way such data is used and the procedures for exercising their rights.[63] This requirement is similar to that provided under the US COPPA. Under COPPA, online service provider must not only provide notice on the website on the kind of information collected from children and how they are used, but also obtain verifiable parental consent for the processing of such information.[64] The service provider must also afford the parent / legal guardian an opportunity the access and exercise data rights (such as prevent further processing, deletion) on behalf of a child.[65] Different from the GDPL, under COPPA, a child is a person of under 13 years.[66] Hence it excludes adolescents. Data Protection Authorities (DPAs) have also a role in the protection of children's personal data. For example, Article 57 of the GDPR requires DPAs to create awareness programs that are specifically modelled for children.[67] COPPA takes an 'incentive' approach. It acknowledges and approve data controllers (ISPs) who implement child specific protection in accordance with COPPA regulations.[68] The Commission's approval can be used as a defense before a court in cases brought against the data controller for violation of COPPA and its regulations.[69]

Conclusion, Strategic Directions and Recommendations

As previously noted on section 3.0. above, protection of children's data and privacy is not as straight forward as that of an adult. Their protection requires a meticulous approach that consider, not just their age, and their vulnerability, but also mental maturity/capability (as this is not determined by age alone) and the right to have a say on matters affecting their rights and which could alter their future.

In 1992, the Royal Government of Cambodia became a party to the Convention of the Rights of the Child (and its optional protocols, i.e the Optional Protocol on the sale of children on 30 June 2002, and to the Optional Protocol on the Involvement of Children in Armed Conflict on 16 August 2006). This Convention, according to Article 31 of the Constitution of Cambodia, has a direct application in the country. Additionally, Article 48 of the Constitution reiterates its commitment to protect children stating;

> *"the State shall guarantee and protect the rights of children as stipulated in the Convention on the Rights of the Child"*

The Royal Government of Cambodia has already taken commendable measures towards guaranteeing and protecting children's rights in the country. Some of the notable measures including the establishment of the strike force to combat internet-based crimes committed against children, namely, the Internet Crimes Against Children (ICAC), adopting guidelines and policies for

63 Article 14 (2) of the Brazilian General Data Protection Law of 2019.
64 15 U.S. Code § 6502 Subsection (b) (1) (A)(ii) and (B).
65 15 U.S. Code § 6502 Subsection (b) (1)(B)(i-iii).
66 15 U.S. Code § 6501 Section (1) defines a child to mean "an individual under the age of 13."
67 Article 57 (3) GDPR.
68 15 U.S. Code § 6503 Subsection (b)(1)(2).
69 15 U.S. Code § 6504 Subsection (b)(3) states; "Upon application to the court, a person whose self-regulatory guidelines have been approved by the Commission and are relied upon as a defense by any defendant to a proceeding under this section may file amicus curiae in that proceeding."

the protection and to support children and youth participation in the protection of their rights[70], and on child protection system[71], as well as establishing a dedicated council to oversee children rights, namely, Cambodia National Council for Children.

However, most of the efforts and data on achievements exclude the protection of children and youth personal data and privacy.[72] This is calls for more action in protecting children and youth personal data and privacy, especially at this day and age where data can (as is being) be used to determine the extent of an individual access to other civic rights and their participation in their communities. Unfortunately, the country has yet to establish a comprehensive data protection framework. Such is necessary to provide for specific rights and protection on children's personal data and privacy. While I acknowledge the government efforts in recognizing the right to personal data protection, privacy and security as provided under the Article 10 of the Civil Code[73], Articles 301, 302[74], and 427[75] of the Penal Code, Chapter 6 of the 2019 E-Commerce law which provided for a framework for consumer protection, Sub-Decree No. 252 on the Management, Use, and Protection of Personal Identification Data[76]. Unfortunately, these efforts are too scattered and not concise enough to sufficiently protect personal data and privacy, especially in the digital era. Luckily, the country is heading to the right direction, amidst in a slow pace. Notably, is the 2021 announcement by the Ministry of Communication to the effect that it is working on a draft data protection law. In support if this move, this research makes the following s strategic directions and recommendations with regards to a framework for the protection of children and adolescents' personal data.

These recommendations take cue of several legal frameworks for the protection of personal data across the globe and pointing out specific considerations in ensuring children and adolescents receive proper protection in line with international blueprint for the protection of a child – the CRC. According the Articles 3 (2) and 4 of the CRC, countries implementing this Convention "shall take all appropriate legislative and administrative measures" to ensure children and adolescent receive sufficient protections. The Royal Government of Cambodia made a commitment to implement this requirement (among others), specifically by enacting Article 48 of the Constitution which states;

70 The Royal Government of Cambodia - National Council of Children, "Decision on Guideline for Applying Child Participation", 2014, https://extranet.who.int/mindbank/download_file/7262/7cd40c1e87f3309afa01b4ace90f1968b0f-7c6ec;
The Royal Government of Cambodia - Ministry of Social Affairs, Veterans and Youth Rehabilitation, "Standards and Guidelines for the Care, Support and Protection of Orphans and Vulnerable Children", 2011, https://extranet.who.int/mindbank/download_file/5511/d2929fab3615a6784b798c01f6680cbfec028f8b;
The Royal Government of Cambodia - Ministry of Education, Youth and Sports, "National Policy on Youth Development", 2011, https://extranet.who.int/mindbank/download_file/4439/d702a6e54358ce6daf65f42eed7f94a79466d6a3; all the sources were accessed on 10.07.2024.

71 The Royal Government of Cambodia – Cambodia National Council for Children, "National Policy on Child Protection System (2019-2029), https://policypulse.org/wp-content/uploads/2020/06/National-Policy-on-the-Child-Protection-System.pdf accessed on 10.07.2024.

72 These efforts are mainly directed to combat child marriages, child labour, protect children with disability, affected with HIV/AIDS, street children and orphans, child trafficking, and child violence as well as improving corresponding (administrative) systems. Cf. UNICEF, A Statistical Profile of Child Protection in Cambodia, 2018, https://bettercarenetwork.org/sites/default/files/Cambodia_Report_Final_web_ready_HIGH.pdf, accessed on 10.07.2024.

73 Providing for the right to privacy, to life, to personal safety, to freedom, to identity, and dignity.

74 Prohibiting interception or recording of private conversations, or recording a person's image in a private location, without their consent. Note: Consent is presumed to be given if the concerned person does not object to the notification of the interception or recording.

75 Prohibiting fraudulently accesses or maintains access to automated data processing systems.

76 Adopted in 2021, this Decree is limited to protecting personal data owned by the Ministry of Information. https://data.opendevelopmentcambodia.net/en/dataset/286af641-68d2-48dd-af64-c233970208e0/resource/e65a252c-5cc7-4d2e-83be-c503eae270cf/download/___.pdf accessed on 10.07.2024.

> *Article 48 : The State shall protect the rights of children as stipulated in the Convention on Children, in particular, the right to life, education, protection during wartime, and from economic or sexual exploitation.*

The State shall protect children from acts that are injurious to their educational opportunities, health and welfare. The first step is for the Royal Government of Cambodia to establish a comprehensive framework for the protection of personal data. Specifically on children and adolescents, the Government should take a special consideration when designing the following aspects:

On Parental Consent

Most data protection frameworks designate a parent or a legal guardian as a person to give consent for the processing of a child or an adolescent personal data. Legal frameworks that rely solely on parental consent for the processing of children's data are lacking. In fact, this approach may contribute to further misuse and infringement of data related and privacy rights of children. An example is the sharenting practices. In addition, these frameworks, as seen in this chapter, lack clear rules and conditions for access rights when processing children's data. In this regard, it is recommended that:

> *i) Laws should explicitly provide for rules for the processing of children's data, on other bases beyond parental consent. A good example is the 'mini framework' established under Part C of the South Africa POPIA. A Part that provides for legal bases, rules, and conditions for the processing of children's data beyond parental consent.*
>
> *ii) To ensure child's best interest, an oversight mechanism should be established to verify parental consent (of lack thereof) against child best interest. This may also (especially) be necessary to regulate sharenting behaviors. An example can be taken from Algeria and Tunisia where a judge of a family court can act as a patron in protecting the best interest of a child. A judge can consent or withdraw parental consent whenever child's best interest dictates so.*
>
> *Another approach would be condition 'child best interest' as the primary consideration in deciding the legality of data processing activities involving children's data. Kenya and Brazil created such a framework and could be taken as an example in legislating this aspect. This approach could be implemented strategically to protect children's data. The requirement to ensure child's best interest is promoted is an obligation embedded in Article 3 (1) of the CRC. An obligation which the Royal Government of Cambodia took commitment to fulfil.*
>
> *iii) Capacity building, as advocated by privacy and child safety online advocates, is an important aspect in protecting children's data. Data protection frameworks should be created to support capacity building to both parents and children. As the opinioned by Jasmontaite and De Hert, both children and parents need to be educated to enable them navigate and adjust [at least] online platforms privacy settings. An example of such requirement is Article 57(1)(b) and subsection 3 of the GDPR has a duty to provide public awareness "free of charge". The provision insists that issues affecting "children shall receive specific attention."*

South Africa POPIA does not give specific mention of children issues but it obligates the Information Regulator to educate the public and advice data subjects on exercising their rights.[77] *A similar provision is provided under Section 8(1)(g) of the Kenya Data Protection Act*

On Age

Defining an age (age group) of children and adolescent afforded special protection is an important aspect in protecting their personal data. Age specifications in the data protection frameworks discussed in this chapter vary substantially. The GDPR specifies the age of 16 as requiring parental consent while under the US COPPA it is up until 13 years. In both cases, there is a protection (or lack thereof) gap between a child (whose data processing requires parental consent) and young adults from 17 to 18 or 14-18/21 respectively. Under these laws, this group of your adult are neither children nor adults for purposes of processing personal data. Or maybe it could also mean what Jasmontaite and De Hert claim, that "they would have to provide consent in the same way as adults".

It is not only crucial for laws to specify age (of a child) but to also consider vulnerability of young adults (adolescents) who also need special consideration. In fact, child specific laws, young adults (up to 18 or 21 as the case may be) are covered by the rules created to protect children. Why should this not be the case in the protection of their personal data, including their privacy, identity and personality?

The Brazil GDPL illustrates an inclusive approach to the protection of children and young adults. As explain on the previous section 4.2 above, the law categorically identifies children and adolescent as a group that is entitled to special protection. Before their data is processed, data controller or processor must ensure child's best interest is maintained.

Governments should, therefore, adopt legislation or put in place policies that require Internet service providers, search engines, social media networks and other providers of Internet enabled content and services to provide children with proper information – adapted to their capacities – about the processing of their personal data and their rights as data subjects. Such providers should also be required to ensure greater transparency of the personal data processing that they carry out. A good example in the right direction is the GDPR, article 12(1) of which requires all companies and public authorities that collect and process personal data to provide information to data subjects (i.e. users) "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child"[78]
As emphasized by (Livingstone, Carr and Byrne, 2016) that children rights in the digital age goes beyond adherence to human rights and values. It embodies empowerment and participation of "child users that fosters their creativity, innovation and societal engagement and development of digital literacy".[79]

Differential Approach and Child Participation

The role of a child in the protection of its personal data should take a more subjective approach. Instead of rigidly depend on just the age, the rules should be flexible enough to allow an assessment of child's maturity (evolving capabilities) and understanding. Accordingly, if a child is considered mature and able to understand the risks and navigate risk mitigations, there should

77 Section 40(1)(a) of the POPIA.
78 Cf. Article 16 of the GDPR and Mario Viola de Azevedo Cunha, "Child Privacy," 13.
79 Cf. Mario Viola de Azevedo Cunha, "Child Privacy,"14.

be no need for parental consent. In such a case, parental involvement should be in terms of direction and guidance. Thereafter, a decision to consent or withheld consent should be left to the child.

This approach is also recommended under Convention on the Rights of the Child (CRC). CRC promote the idea of a parent to direct and guide a child (depending on their level of maturity and understanding) and let them exercise their own rights.[80] Article 12 (1) of the CRC states;
"States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child."

Of course, the CRC also recognize cultural and social nuances of specific communities in legislating for such a framework. Nevertheless, a balance needs to be created to avoid robbing children and adolescent of their right to decide on matters affecting their rights and identities.

In this respect, the Royal Government of Cambodia has already taken steps to increase participation of adolescents and youth representatives in decision making process affecting their lives at local and national level events. However, according to World Vision, these activities tend to be ad-hoc and one-offs.[81] Nevertheless, I believe this is a good start in creating permanent youth participatory system where they can be able to speak and shape policy dialogues pertaining their rights, such as the right to data protection and privacy. Such a system would also implement policy statement 5.6 and action statement 6.1 item 1 of the National Policy on Youth Development of 2011.

A complete reliance on a parental consent in protecting children's personal data and privacy not only denies them the ability to know data processing activities involving their data (example through sharenting), but also an opportunity to take part into decisions that affect their rights. Eventually, children are unaware of the type of data and nature of processing activities involving their data that continue to take place on and offline. Also, in situation where a child is considered immature to make decisions affecting their (data protection and privacy) rights, rules should be made to obligate parents to, at least, consult a child before they either process personal data of their children, or consent to processing activities by others. Following the opinion of A29WP, a framework that allows for "parallel or joint consent of the child and a parent, or even to the autonomous consent of a mature child" is legislative viable.[82]

80 Article 5 states;
"States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention". of Convention on the Rights of the Child adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989.
See also Article 13 (1) of the CRC which states;
"The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice".

81 World Vision, "Increase in Children and Adolescents Who are Protected from All Forms of Violence and Participating in Decision Making", Fact Sheet- Cambodia, (February 2023), https://reliefweb.int/attachments/b9efc595-f12e-4c66-9e2e-b4ccf2e84a53/CHILD%20PROTECTION%20AND%20PARTICIPATION%20Pramme%20Factsheet-min.pdf accessed on 10.07.2024.

82 Article 29 Working Party (A29WP), "Opinion 2/2009 on the Protection of Children's Personal Data: (General Guidelines and the Special Case of Schools," (WP 160), 11 February 2009]:6 < Cram Rhône-Alpes (europa.eu)> accessed 22.09.2023.

Instead of a one-size-fits-all approach, protection of children's data and privacy should take a differential approach. Beyond specifying age categories, (which should also consider adolescents) rules on the protection of children's data and privacy should take cognizance of children developmental variances and distinct susceptibilities. An opinion by the Article 29 Working Party suggests, "parental consent may be required to process the personal data of children below a certain age (e.g. 13 years); above this age threshold, parental intervention may be replaced by specific safeguards that reflect children's age of capacity."[83] Terri Dowty and Douwe Korff suggest, a proper framework should take cognizance of "both subjective matters such as the maturity of the minor and more objective matters such as whether the matter for which consent was given was in the direct interest of the minor or not, and indeed whether the parents were, or should have been involved."[84]

Brazil GDPL attempted to legislate this aspect. Section 14(6) illustrates the need to consider, not just children's vulnerability, but also their mental maturity and understanding. In the context of user information/privacy policies, the law states, "taking into account the physical-motor, perceptive, sensorial, intellectual and mental characteristics of the user, using audiovisual resources when appropriate, in order to provide the necessary information to the parents or the legal representative and that is appropriate for the children's understanding." This understanding can be extended to other aspects such as the ability of a child to consent and exercise other (data related) rights.

On Processing Obligations

The law should set out specific obligations to data controller (and processors) towards the protection of children personal data. Moreso, Online/Internet Service Provider (O/ISPs) should be obligated to set up online privacy policies and technical settings to meet children needs and understanding. For example, the GDPR, COPPA, Brazil GDPL. These should be transparent and clear enough for children and parents – highlighting the nature of processing activities involving children's data.

An additional requirement could be added for O/ISPs to send annual notices to children and parents whose data is being processed. This approach has been considered under the FERPA (USA). Such notice reminds children and parents of their rights to access and other ancillary rights tied to the processing of (children) data.

83 Article 29 Working Party (A29WP), "Opinion 2/2009 on the Protection of Children's Personal Data: (General Guidelines and the Special Case of Schools," (WP 160), 11 February 2009]:6 < Cram Rhône-Alpes (europa.eu)> accessed 22.09.2023.

84 Terri Dowty and Douwe Korff, "Protecting the Virtual Child:The Law and Children's Consent to Sharing Personal Data,"(Study prepared for ARCH–action on rights for Children- and the Nuffield Foundation), 2009 <Protecting20the20virtual20child.pdf (nuffieldfoundation.org)> accessed 22.09.2023.

PART II
CYBERSECURITY

Cybersecurity

Designing a Cybersecurity Legal Framework for Cambodia

Professor Phallack Kong

Abstract

As Cambodia embarks her journey of digital transformation, the dependency on digital technologies become increasing, thus Cybersecurity risks management is important for the country to ensure the continuity of essential services provided by organization of critical infrastructure in the country. Envisioning the digital technologies will bring to Cambodia opportunities for economic growth, improvement of public services, and citizens' well-being as well as international integration, Cambodia's readiness to build the trustworthiness in digital system is still in infant stage in particular cybersecurity management due to increasing of cyberattacks, data breaches, and digital espionage, etc. Therefore, this paper is prepared to outline challenges and policies adopted by Cambodia aiming to address them and prepare Cambodia for future digital readiness; and propose legal framework on cybersecurity management and recommends for implementation of cybersecurity law.

Challenges and Polices Response to Building the Trustworthiness in Digital system

Cambodia's readiness to digital adoption and digital transformation remains challenging, despite recent growth of the information and communication technology (ICT) system. The challenges include i). digital connectivity, ii). FinTech Infrastructure, iii). digital payment systems, iv). logistics and last-mile delivery to support digital social economic development process, v). legal framework and cybersecurity management, vi). technology competency of citizen including knowledge and skills and leadership in digital sectors are limited and required strong commitment and policy support in order to make Cambodia become a competitive country in the region and globally in the era of emerging technologies such as artificial intelligence, blockchain, Augmented Reality and Virtual Reality (AR&VR), Cloud Computing, Big Data, Internet of Things (IoT), Robotic Processor Automation (RPA), Intelligent Apps (I-Apps) or smart app, etc.

To tackle these challenges, the Cambodia government introduced the Digital Economy and Society Policy Framework 2021-2035 (DESPF), Cambodia Digital Government Policy 2022-2035 (CDGC) and Pentagonal Strategy Phase 1 (PSP1). The DESPF determines 139 policy measures and takes into account the possible negative effects of the presence and use of technologies aiming to achieve the goals of building a Cambodian digital economy and society. The CDGC identifies 83 priorities actions aiming to improve quality of life and building trust among citizens through better public services provisions. The PSP1, the socio-economic policy agenda of the second generation of the Cambodian government (CG2) of the 7th Legislature of the National Assembly which prioritizes 5 key areas such as People, Road, Water, Electricity and Technology. The core of PSP1 is governance and modernization of state institutions, and the 5 strategic pentagons are Human Capital Development (Pentagon 1); Economic Diversification and Competitiveness Enhancement (Pentagon 2); Development of Private Sector and Employment (Pentagon 3); Resilient, Sustainable and Inclusive Development (Pentagon 4); and Development of Digital Economy and Society (Pentagon 5).

In a nut shell, these three policy documents set out the vision of "building a vibrant digital economy and society to accelerate new economic growth and promote social well-being in order to realize Cambodia Vision 2050. If the DESPF and the CDGC are successfully implemented through the developing infrastructures to enable digital transformation and building digital reliability and confidence in digital system, by a 2035, the level of maturity of three pillars of digital economy and society including digital government, digital businesses and digital citizens will be realized to the certain extents. This paper does not explain all policy measures and priorities described in those policies, but focus on designing Laws and Regulations for digital economy and society aiming at strengthening the management of digital security in Cambodia in particular law on cybersecurity which is described in the following section.

Designing Cybersecurity Legal Framework for Cambodia

As increasing the use technology by the governments, businesses and citizens, enormous potential cyberattacks and cybersecurity incidents become more sophisticated and dangerous. Governments around the globe including Cambodian government take into account in development of legal framework and mechanism on cybersecurity management of their respective country. This section explains the development of cybersecurity law in Cambodia and key provisions of the draft law. It is a personal opinion of the author. It neither represent the position of the Working Group of Drafting Cybersecurity Law nor the Ministry of Post and Telecommunications.

The DESPF directs the development of laws and regulations and policies or strategies on Cybersecurity, Data protection and Privacy, Public Information Law, Cybercrime Law, Trade Secrets and Non-disclosure Information Law, E-commerce User Ethics Law and amendment of relevant laws and regulations related to cybersecurity. Furthermore, the DESPF recommends the capacity building plan on digital knowledge for lawmakers and technical staffs, raising public awareness, developing and investing in infrastructures and national cybersecurity management systems, establishing institutional mechanisms in line ministries at both national and sub-national levels including focal point for the exchange of information on threats and risks, establishing standards, technical frameworks, and response procedures in developing digital systems and infrastructure which are resilient against attacks, developing strategies and guidelines to raise awareness of the levels of the cybersecurity threats, promoting cybersecurity skills development, and establishing bilateral and multilateral cooperation with international organizations or associations and the private sector related to cybersecurity to share information, experiences and best practices. [1]
The statement outlined in the preceding paragraph and three main policies mentioned in this article as well laws and regulations enforced in Cambodia build as a basis for the development of the draft law on cybersecurity. Additionally, number of Laws, policies, strategies, reports, research papers related to cybersecurity of the United Nations, International Telecommunication Union, ASEAN, EU, international organizations and selected countries such as Estonia, Singapore, Japan, Australia, Thailand, Vietnam, Malaysia, USA, China, Taiwan, South Korea, etc. are consulted. The draft law on cybersecurity was circulated for inputs from critical information infrastructure organizations or companies providing essential services in and to Cambodia. At the time of writing, the draft law on cybersecurity is reviewed by the technical working group of the Office of the Council of Ministers.

Purpose and Scope of the Draft Law on Cybersecurity (DLC)

The DLC aims to protect Cambodia's digital space by managing cybersecurity risks. It also seeks to build trust in digital technology, which is crucial for the growth of the digital economy. The DLC applies to Critical Information Infrastructure Organizations (CIIOs) and other relevant individuals or entities. These are organizations that provide essential services, such as telecommunications, finance, and energy, etc. and whose disruption could have a significant impact on the country.

The Governmental Entities in Charge of Cybersecurity Management

The DLC outlines the government entities responsible for managing cybersecurity in Cambodia. It establishes their roles, responsibilities, and the overall structure for cybersecurity governance. The Digital Security Committee (DSC) is the highest authority for cybersecurity in Cambodia led by the Prime Minister, a permanent vice chairman ranked as Deputy Prime Minister, 4 vice chairmen (Minister of Economy and Finance, Minister of Interior, Minister of National Defense and Minister of Post and Telecommunications), 6 members in which 3 Secretaries of State respectively representing Office of the Council of Ministers, Ministry of Foreign Affairs and International

1 Ibid 1, pp. 70-75

Cooperation and Ministry of Justice , Commander-in-Chief of the Royal Cambodian Armed Forces, General Commissioner of National Police, and Commander of the National Gendarmerie. The DSC may add additional members as Vice-Chairmen or members representing other relevant ministries-institutions as necessary.

The DSC is entrusted to lead, coordinate and promote the management of digital security to protect the interests of all social actors against all forms of attacks as to respond to all technical aspects and relevant forces and thereby maintaining and protecting digital security. The Organization and functioning of the DSC is determined by Sub-Decree. The DSC is supported by the General Secretariat led by the Minister of Post and Telecommunications. The General Secretariat of the D.S.C. is structured into Cambodian Cybersecurity Unit under the jurisdiction of the Ministry of Post and Telecommunications, Anti-Cybercrime Unit under the jurisdiction of the Ministry of Interior, Cyber defense Unit under the jurisdiction of the Ministry of National Defense, Cyber diplomacy Unit under the jurisdiction of the Ministry of Ministry of Foreign Affairs and International Cooperation, and a Secretariat.

As stipulated by the Sub-decree, the Organization and functioning of Cambodian Cybersecurity Unit (CCU) is determined by a sub-decree. The CCU-to-be will function as a Cambodian Cybersecurity Authority and it serve as the executive body of the General Secretariat over cybersecurity affairs. Its roles and responsibilities include i) Lead, coordinate, implement and promote the management of cybersecurity affairs in accordance with policies, strategies, laws, and regulations; ii) Lead and coordinate at the technical level and take measures to prevent cybersecurity risks and respond to cybersecurity incidents in both the public and private sectors,; iii) Develop Common Guidelines on Cybersecurity Management and propose the revision and/or amendment of laws, regulations, and policies related to cybersecurity for Digital Security Committee General Secretariat; iv) Inspect and audit the compliance of the implementation of Common Guidelines on Cybersecurity Management and Additional Guidelines on Cybersecurity Management by Sector; v) Serves as the National Computer Emergency Response Team, vi) Manage the operation of Cybersecurity Operation Control System, cybersecurity data, and laboratories for digital forensics related to cybersecurity; vii) Grant, modify, suspend, transfer, or revoke cybersecurity licenses and resolve disputes related to cybersecurity determined in this law and related regulations, viii) Prepare a cybersecurity exercise and/or Vulnerability Assessment and Penetration Testing on the cybersecurity management systems of the Royal Government and CIIOs in order to assess the resiliency of the national cybersecurity management system and the cybersecurity management systems of CIIOs with coordination from General Secretariat, ix) Coordinate and promote local and international cooperation related to cybersecurity, x) Prepare awareness programs and promote cybersecurity professional skills training; xi) Make reports and recommendations related to cybersecurity affairs to the General Secretariat; and xii) Perform other roles and duties as assigned by the General Secretariat.

Despite having the DSC, the General Secretariat, the DLC requires a cooperation from the relevant Ministries and institutions especially those have functions as the CIIOs and manage CIIOs.

Critical Information Infrastructure Organizations (CIIOs)

The DCL determines two types of CIIOs, the regular CIIOs and the CIIOs with characteristics of national significance. The former includes CIIOs in the public sector providing essential services in sectors such as energy, transport, banking and finance, health, water supply and distribution, communications, digital infrastructure, natural resources, culture, media, and other sectors as determined by separate provisions. The latter is CIIOs whose service provisions are related to national security, public interests, or the interests of the Kingdom of Cambodia such as national defense, national security, diplomacy, national secret information, national data and so on.

The criteria for determining CIIOs, list of essential services, and list of CIIOs are determined by a decision of DSC based on the request of the General Secretariat. Furthermore, the DCL allows DSC to review and/or further designate CIIOs based on the development of society, economy, and technology, actual circumstances within the Kingdom of Cambodia and international trends. The review may take place every 2 (two) years for regular CIIOs and once a year for the CIIOs with characteristics of national significance. The DCL requires a prior consultation with line ministries/institutions for determination and review of CIIOs and essential services.

CIIOs and its essential services determined by the DSC have to fulfill roles and duties prescribed by the DCL namely i) Create a unit in charge of cybersecurity and retain cybersecurity professionals for CIIOs; ii) Develop Internal Regulations on Cybersecurity Management in accordance with Common Guidelines on Cybersecurity Management and Additional Guidelines on Cybersecurity Management by Sector if any; iii) Conduct an annual cybersecurity risk assessment and cybersecurity audit as stated in DCL and provide the reports to the CCU; iv) Monitor, identify, analyze, and evaluate cybersecurity risks on a regular basis and classify the types of cybersecurity risks based on their levels in order to take measures to prevent and mitigate cybersecurity risks in accordance with Common Guidelines on Cybersecurity Management; v) Take measures to prevent, mitigate, and resolve cybersecurity incidents based on the types and levels in accordance with Common Guidelines on Cybersecurity Management; vi) Notify cybersecurity incidents as required the DCL; vii) Participate in cybersecurity exercises and/or Vulnerability Assessment and Penetration Testing on its cybersecurity management system in order to assess the resiliency of the cybersecurity management system with coordination from General Secretariat; viii) Organize cybersecurity training and awareness raising for employees, customers, and business partners; ix) Cooperate with ministries/institutions and relevant stakeholders to manage cybersecurity risks; and x) Perform other roles and duties as determined by the DCL and related regulations.

Guidelines on Cybersecurity Management

The DCL outlines the three layers of cybersecurity management rules. The first layer or foundational layer is called Common Guidelines on Cybersecurity Management. The guidelines set minimum requirements for all CIIOs and determined by a sub-decree. The second layer is called Sectoral Guideline or Additional Guidelines on Cybersecurity Management developed and determined by line ministries and institutions in consultation with the General Secretariat. This sectoral guideline is developed is only the line ministries and institutions think it is necessary and avoids creating additional burden for industries. For example, the National Bank of Cambodia's Technology Risk Management Guidelines (July 2019). Banking sector advanced in building trustworthiness in its core banking system for its operation and consumers. And the third layer is Internal Regulations on Cybersecurity Management of the CIIOs or Manual of Cybersecurity Management Policies, Standards and Procedures of CIIOs. This guideline or manual is a "Must-DO" and decided by the management body or senior executives of CIIOs. In addition, it must be consistent with Common Guidelines on Cybersecurity Management and Additional Guidelines on Cybersecurity Management by Sector if any.

The DCL does not require CIIOs to choose and adopt any specific technology, software, equipment or standards of cybersecurity management. However, CIIOs must comply with laws and regulations of the Kingdom of Cambodia and treaties and agreements, etc. ratified by Cambodia. To avoid any risks taking of non-compliance, CIIOs should consult with General Secretariat and/or line ministries and institutions having jurisdiction over the business activities.

Cybersecurity Risk Management

The DCL requires CIIOs to conduct a cybersecurity risk assessment at least 1 (one) time per year and cybersecurity audit at least 1 (one) time every 2 (two) years. CIIOs are not permitted to retain

the same cybersecurity risk assessor for more than 3 (three) years consecutively and the same cybersecurity auditor for more than 6 (six) years consecutively. The Report on cybersecurity risk assessment and Report on cybersecurity audit are required to submit to the CCU within 7 (seven) working days after its completion.

The DCL requires the CIIOs to provide the names and information of the cybersecurity professional in charge to the CCU within 30 (thirty) working days after being designated as a CIIO. The DCL instructs CIIOs to rectify their cybersecurity management system if it is vulnerable and can lead to cybersecurity incidents and the cybersecurity management system of the CIIOs is not in compliance with Common Guidelines on Cybersecurity Management and Additional Guidelines on Cybersecurity Management by Sector if any.

Reporting of cybersecurity incidents is a MUST. The DCL requires CIIOs to immediately notify the CCU and persons affected by the cybersecurity incident from the time when the CIIOs learn of the cybersecurity incident of serious impact and within 12 (twelve) to 72 (seventy-two) hours from the time when the CIIO learns of the general cybersecurity incidents. The CIIO that is unable to prevent, mitigate, or resolve the impact of the cybersecurity incident on their own, can make re request to the CCU for support or intervention. However, all costs are to be borne by the requesting CIIO.

Cybersecurity Services, Cybersecurity Professionals, Cybersecurity Development Fund and Investment Incentives

The DCL requires cybersecurity service providers to apply for a license providing cybersecurity services in the Kingdom of Cambodia. Detail Conditions, formalities, and procedures on granting a license providing cybersecurity services are determined by a Prakas of the Minister of the Ministry of Post and Telecommunications. Besides that, cybersecurity professionals are required to register in the registry of the Cambodia Digital Profession Board, pay membership fee and obtain a license to practice cybersecurity.

The DCL proposes the establishment of the Cybersecurity Development Fund aiming for research, development, and awareness raising of cybersecurity as well as cybersecurity risk management in the Kingdom of Cambodia. Any cybersecurity service providers receive a license providing cybersecurity services is requires to contribute 2(two) percent of gross revenue to the Cybersecurity Development Fund. The Ministry of Post and Telecommunications will act as the executive body of the Royal Government of Cambodia to establish, manage, monitor, and evaluate the use of the Cybersecurity Development Fund in accordance with this law and other applicable laws and regulations.

Besides, the sticks, the DCL provides incentives for Investment activities related to software development that supports the telecommunications sector and information and communication technology sector related to cybersecurity in accordance with the Law on Investment of the Kingdom of Cambodia and relevant regulations or decisions of the Royal Government based on a request of Ministry of Post and Telecommunications.

Cybersecurity Inspection, Cybersecurity Dispute Resolution and Penalties

As part of the Cambodian legislation structure, Cybersecurity Inspection, Cybersecurity Dispute Resolution and Penalties are outlined in the DCL.

The Minister of Ministry of Post and Telecommunications appoint Cybersecurity Inspection Officers to monitor, investigate, gather evidence, and strengthen the enforcement of cybersecurity law. Cybersecurity Inspection Officers receive legal status as judicial police to monitor offenses as stated

in the cybersecurity law and act in accordance with provisions of the Criminal Procedure Code. The DCL establishes administrative complaint procedures against the Cybersecurity Inspection Officers. Any person who does not agree with any action taken by a Cybersecurity Inspection Officer may file a complaint to Ministry of Post and Telecommunications within 30 (thirty) days from the date of receipt of the decision. The Minister of Ministry of Post and Telecommunications is mandated to issue a decision on the complaint within 45 (forty-five) days from the date of receipt of the complaint. If such a person does not agree with the decision of the Minister of Ministry of Post and Telecommunications, he or she may file a complaint to other mechanisms of the Royal Government or to the court according to procedures.

Besides criminal offenses, all disputes related to cybersecurity affairs, a disputing party is required to file a complaint to the CCU for a resolution in accordance with existing procedures. The DCL requires the CCU to conduct a conciliation or resolution of a dispute related to within 15 (fifteen) days and the result of the conciliation is recorded in a conciliation report. If the conciliation fails, CCU is require to refer the dispute to the Minister of the Ministry of Post and Telecommunications in order to be resolved according to procedure.

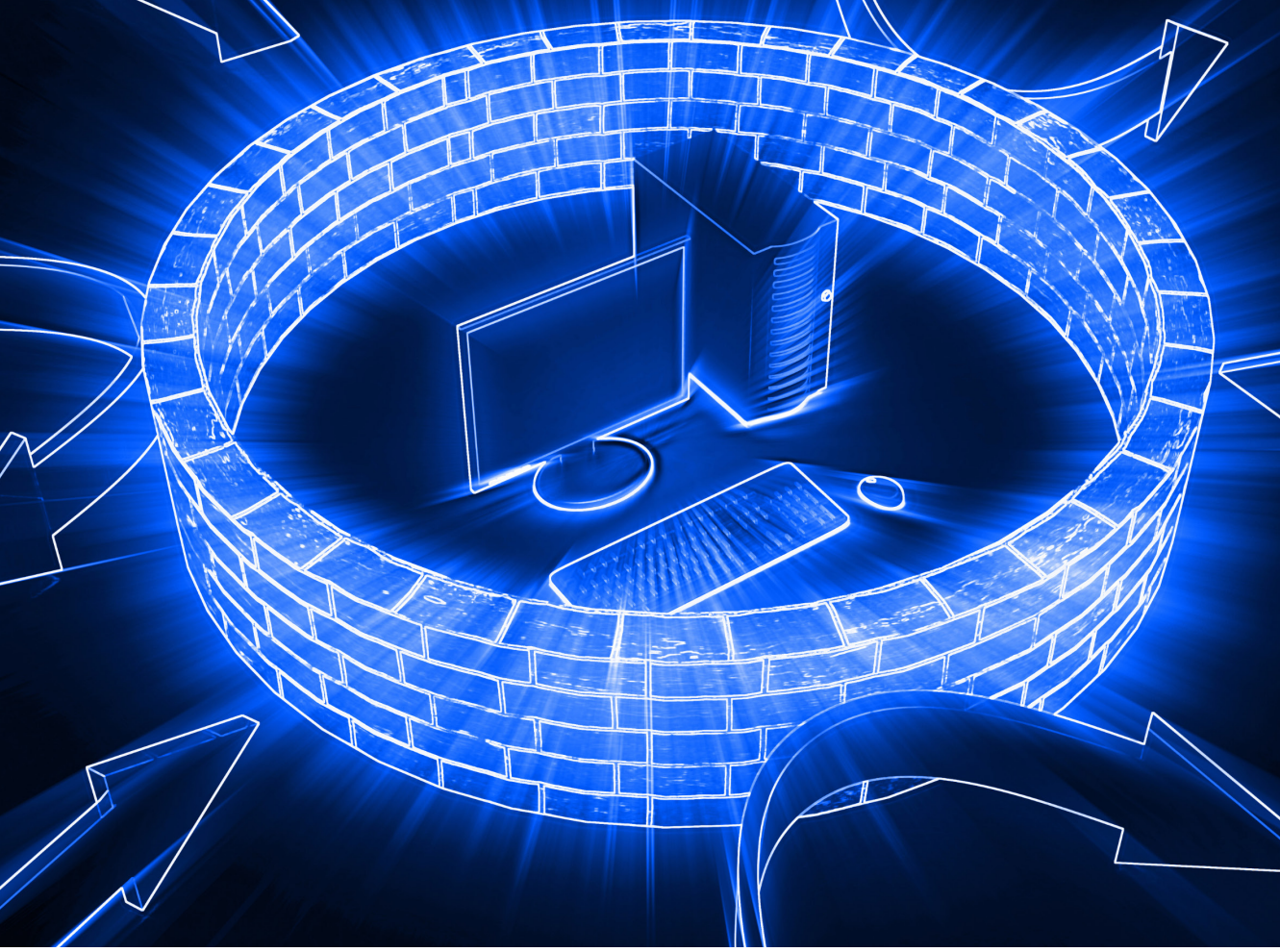
The DCL defines two types of penalties such as administrative penalties and criminal penalties. The former includes written warning, fine, restriction, suspension, or revocation of license and other administrative punishments, and the latter includes criminal penalties determined the law and other criminal provisions of other laws. Any CIIOs violate provisions of cybersecurity law will be subjected to either administrative penalties or criminal penalties depending on nature of offense and number of repetition of offenses.

Conclusion and Recommendations

As explained above, the DCL was developed based on laws and policies across the globe with the purpose to have a harmonious cybersecurity legal framework but reflecting the Cambodia's political economy and context.

The DCL sets 2 (two) years of grace period of preparation for the implementation of the law. This period allows the government and all CIIOs to work together and develop an effective cybersecurity implementation plan and mechanisms. That means the law will come into force after two years from the date of promulgation. The DCL is expected to be passed within the mandate of the government of the 7th Legislature of the National Assembly.

The proposed implementation plan for the adopted cybersecurity law includes i) formulating implementation regulations, ii) developing the national strategy on civilian cybersecurity management and national defense cybersecurity management , iii) developing cybersecurity skills through education and awareness raising programs for government, private sector and citizens to build culture of cybersecurity, iv) establishing a public private partnership between the government, private sector, academia, civil societies and international organizations to share resources, information and best practice of tackling cybersecurity challenges, v) setting the security operation center, preparation and implementation of risk management program or framework, and vi) conducting a voluntary cybersecurity risks assessment to test the resiliency of the system, etc..



Cybersecurity

Digital Security in the European Union – Regulations and the Future of Digital Security and Resilience

Ferdinand Gehringer

Introduction

With the Network and Information Security Directive 1.0 (NIS-1 Directive)[1] in 2016, the European Union has for the first time issued an EU-wide directive on cybersecurity and resilience. At that time, not all countries had enacted an cybersecurity law or a cybersecurity strategy. It was intended to improve cybersecurity throughout the EU and strengthen cooperation between member states - a late and already overdue step at the time. Given the advanced level of digitalization and interconnection of facilities and services within the European Union, a cybersecurity regulation would have been opportune at an earlier stage.

Since then, European Member States have made significant progress in increasing cyber resilience. For example, the NIS-1 Directive has changed awareness of the importance of cybersecurity. States have created a national framework for information security and created cybersecurity strategies where these were not yet in place. They have also created national capacities and implemented regulatory measures. It also strengthened cooperation at Union level through the establishment of the Cooperation Group and the network of national cybersecurity incident response teams. However, these developments should not hide the fact that there are still significant shortcomings in the level of protection at Union level.

The European Union has now reacted to this once again and is striving to further harmonize the legal framework to increase the level of protection.

In 2019, the European Union presented the programme for the Digital Decade up to 2030. In the European Union's Digital Decade program security plays an overriding role.[2] In order to strengthen cybersecurity more effectively while increasing digitization within the Union, numerous regulations and legislative projects have been implemented, launched or are currently being planned in recent years and months.

In 2020, the EU Commission and the European External Action Service presented the new European Cybersecurity Strategy[3] as a part of the Digital Decade. The strategy includes the Network and Information Security Directive 2.0 (NIS-2 Directive)[4], which replaces the currently applicable NIS-1 Directive, and the Critical Entities Resilience (CER Directive)[5]. In addition, the Digital Operational Resilience Act (DORA)[6] was passed. A few selected regulations and projects will be used below to illustrate the European Union's approach to digital protection and the content of the regulations, especially for critical infrastructures.

1 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.

2 European Commission, Europe's Digital Decade: digital targets for 2030, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en,

3 European Commission, The EU's Cybersecurity Strategy for the Digital Decade, https://ec.europa.eu/newsroom/dae/redirection/document/72164.

4 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

5 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557.

6 Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending regulations (EC) NO 1060/2009, (EU) NO 648/2012, (EU) NO 600/2014, (EU) NO 909/2014 AND (EU) 2016/1011, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_41_2022_REV_1.

New and Future Regulations

Digital Protection of Critical Infrastructure through the Network and Information Security Directive 2 (NIS-2 Directive)

The NIS-1 Directive (2016) represented the first cybersecurity legislation at the European Union level. It aimed to establish a common European legal framework, thereby improving cybersecurity capabilities at the national level, and enabling increased cooperation at the EU level. European Union member states were required to establish a strategy for the security of network and information systems. The NIS-1 Directive also introduced security requirements and reporting obligations for operators of essential services and for providers of digital services, a uniform risk management system and created a Computer Security Incident Response Teams (CSIRT)[7] network. These measures were intended to achieve a uniformly high level of security of network and information systems in the EU to improve the functioning of the internal market.

Purpose

The Network and Information Security Directive 2 (NIS-2 Directive)[8] is the further development of the regulation from 2016. The NIS-2 Directive aims to strengthen the resilience of organizations and authorities within the European Union and increase confidence in the European market through uniform cybersecurity standards.

Scope

Thus, it introduces rules and obligations for sharing cybersecurity information. The directive no longer distinguishes between "operators of essential services" and "providers of digital services," but instead defines "essential" and "important entities" of certain sectors. The scope of application is thus expanded compared to the NIS-1 Directive.

"Essential entities" (as defined in Article 3(1) of the NIS-2 Directive) are all entities exceeding a specified threshold of supply that operate in one of the following "high criticality sectors":

- Energy (electricity, district heating, oil, natural gas, hydrogen),
- Transport (air transport, rail transport, shipping, road transport),
- Banking and financial market infrastructures,
- Healthcare,
- Drinking water and waste water,
- Digital infrastructure (including Internet node operators, cloud computing service providers, data center service providers, trust service providers, public electronic communications network and service providers),
- ICT service management,
- Public administration entities,
- Space.

7 A Computer Security Incident Response Team (CSIRT) is a group of IT specialists who advise and assist an organization in the assessment, management and prevention of cybersecurity emergencies and coordinate incident response activities.

8 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

In addition, essential entities also include the following:

- all providers of qualified trust services and top-level domain name registries, regardless of their size, as well as DNS service providers,
- other entities of the type listed in Annex I or II that have been classified by a Member State as an "essential entity",
- Entities classified as critical entities under Directive (EU) 2022/2557 ("Critical Infrastructure Resilience Directive"),
- Operator of essential services under the NIS Directive.

Accordingly, "major establishments" (as defined in Article 3(2) of the NIS-2 Directive) are all other undertakings active in one of the sectors listed in Annex I or Annex II (other critical sectors). This includes those entities that fall into one of the sectors but do not exceed the required threshold and entities that operate in one of the sectors listed in Annex II. These include:

- Postal and courier services,
- Waste Management,
- Production, manufacture and trade of chemical substances,
- Production, processing and distribution of food,
- Manufacturing industry/production of goods (including manufacturers of medical devices and in-vitro diagnostics, data processing equipment, vehicle manufacturers and mechanical engineering companies),
- Digital service providers (online marketplaces, online search engines and social networks),
- Research.

Regulatory Requirements

The entities covered by the scope are to take appropriate and proportionate technical, operational and organizational measures to ensure the security of network and information systems (Art. 21 of the NIS 2 Directive). Among other things, they are required to establish auditable information security management systems (ISMS) and to expand risk management through extended minimum requirements (guidelines, update and certification requirements, risk management, audits). For example, concepts relating to risk analysis, the management of security incidents, the maintenance and continuation of operations (back-up management, business continuity management and recovery, and crisis management) are required. There will also be an increased focus on personnel security and access controls. Basic cyber hygiene measures, training requirements, multi-factor authentication solutions, encryption, and cryptography are part of the list of requirements directed to member states. The minimum requirements must be implemented according to the state of the art and considering relevant European and international standards and technical specifications.

The response capability to cyber incidents and disruptions is also to be improved. The directive provides for a graduated reporting obligation for security incidents. An early warning is to be issued no later than 24 hours after becoming aware of an incident, followed by an initial assessment within 72 hours. After one month, a final report on the security incident is to be submitted to the national reporting authority.

Through a cooperation group, practical cooperation between member states and public and private sector entities is to be intensified. Regulations and obligations to share information are intended to underpin this. The European Union Agency for Cyber Security (ENISA) is also developing and maintaining a vulnerability database.

Member States are strengthened in their enforcement powers and sanction possibilities[9] and are imposed supervision and enforcement obligations to ensure the implementation of the obligations for the facilities or to be able to sanction them. On-site inspections and spot checks can be carried out, and information and evidence of the implementation of the addressees' obligations can be requested. Member States should also impose coercive sanctions and fines to bring about the implementation of the measures[10]. Violations of a compliant use of risk management measures or of reporting obligations are subject to severe fines: up to EUR 10 million or 2% of total annual turnover for essential facilities, and up to EUR 7 million or 1.4% of total annual turnover for important facilities.
If the competent authority finds that enforcement measures taken are ineffective, it may also require, in respect of an essential facility, that natural persons responsible for management tasks at the executive or board level or at the level of the legal representative are temporarily prohibited from exercising management tasks in accordance with national law.[11]

Implementation

The NIS-2 Directive was finalized as a Union legal act on December 27, 2022, and is currently in the transposition phase into national law. It must be transposed into national law by October 17, 2024, with an implementation period of 18 months, and will then apply in the member states from October 18.

Physical Protection of Critical Infrastructure through the Resilience of Critical Entities Directive (CER Directive)

The Resilience of Critical Entities Directive (CER Directive)[12] on the resilience of critical entities replaces the ECI Directive[13] from 2008.

Purpose

It aimed to protect the energy and transportation sectors across the EU. Following the digital protection of entities anchored and further developed in the NIS directives, the physical protection of critical entities is now to be increased, physical resilience strengthened and vulnerabilities reduced in order to ensure the delivery of services to society and the economy.

Scope

Compared to the European Critical Infrastructure Directive (ECI Directive), the scope of application has been extended considerably. The CER defines the following 11 sectors, most of which coincide with the NIS-2 directive:

- Energy, including electricity, district heating, oil, gas and hydrogen operators,
- Transport by air, rail, water and road, including public transport,
- Banking,
- Financial market infrastructure, including trading venues,

9 Article 32 and Article 33 NIS-2 Directive.
10 Article 34 NIS-2 Directive.
11 Article 32(5)(b) NIS 2 Directive.
12 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557.
13 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114.

- Health, including healthcare providers, basic pharmaceutical product and critical device manufacturers, and research and development of medicinal products,
- Drinking water suppliers and distributors,
- Waste water disposal and treatment,
- Digital infrastructure, including electronic communications services and data centers,
- Public administration entities at the central government level, excluding national security, public security, defense and law enforcement,
- Space operators of ground-based infrastructure,
- Food businesses engaged exclusively in logistics and wholesale distribution and in large-scale industrial production and processing.

Regulatory Requirements

Member States are to conduct a risk assessment to identify critical entities[14], i.e., service providers that are essential for the maintenance of essential functions for society, economic activity, public health and safety, or the environment.[15] By January 17, 2026, a national risk assessment must be conducted for the sectors listed in the CER Annex, and a list of all critical facilities in each sector must be developed by July 17, 2026. The list must be updated every 4 years after a new risk assessment.

Like the member states, critical entities must also conduct an analysis and assessment every 4 years of the risks that could trigger a security incident and jeopardize the provision of their services.[16] This involves natural or man-made risks (all-hazards approach). In addition to hostile threats and terrorist crimes, this also includes accidents, natural disasters, and pandemics. Interdependencies between sectors and cross-border effects must be taken into account accordingly.
To prevent an incident or to limit and manage its consequences, critical entities should take appropriate and proportionate measures, including technical, organizational and security aspects.[17]

The following measures must be documented in a resilience plan within the company, and their implementation must be monitored by a competent authority:

- Disaster risk reduction and climate change adaptation measures,
- Physical access protection for premises, such as fencing, perimeter surveillance, access controls,
- Risk and crisis management procedures and emergency response plans,
- Business continuity measures and identification of alternative supply chains,
- Personnel security management incl. background checks,
- Awareness measures for personnel.

Relevant European and international standards are to be considered in the implementation. The Commission will adopt implementing acts specifying technical and methodological specifications for the measures.

In addition, the CER Directive defines similar reporting requirements as the NIS-2 Directive. It requires immediate reporting to the competent authority of security incidents that may lead to a significant disruption in the provision of essential services.

14 Article 5 CER Directive.
15 Articles 6, 7, and 8 CER Directive.
16 Article 12 CER Directive.
17 Article 13 CER Directive.

In addition, a Critical Facility Resilience Group is designed to facilitate collaboration among Member States, including the sharing of information and best practices. The European Commission offers support for testing the resilience of critical entities.

Implementation

Like the NIS-2 Directive, the legislative process for the CER Directive was completed in December 2022 and the Directive was published in the Official Journal on December 27, 2022. It is currently being transposed into national law, with an implementation deadline of October 17, 2024.

Specific Requirements for the Financial Services Sector with the Digital Operational Resilience Act (DORA).

Digital Operational Resilience Act (DORA)[18] is part of the Digital Finance package[19] and includes measures to further promote the potential of digital finance in terms of innovation and competition while mitigating the associated risks. The DORA regulation underscores the need for financial companies to address the risks posed by digitalization and the accompanying heavy reliance on information and communications technology (ICT) with an appropriate organization and the necessary internal control system (ICS).

Scope

It is a financial services law. For all financial services sectors falling within its scope, it establishes a higher common basis for risks in the area of ICT and creates a coherent framework for the supervision of critical ICT providers ("ICT third parties") for financial institutions. Until now, financial institutions have managed the main categories of operational risk mainly with the allocation of capital.

Regulatory Requirements

The regulation now addresses the fact that ICT incidents and a lack of operational resilience can threaten the stability of the entire financial system, even if "adequate" capital is available for the traditional risk categories. After DORA goes into effect, financial institutions must also follow rules for protection, detection, mitigation, recovery, and restoration capabilities against ICT-related incidents. The regulation explicitly addresses ICT risk and establishes technical standards, rules for ICT risk management, incident reporting, operational resilience testing, and third-party monitoring of ICT risk.

Implementation

As a regulation, DORA applies directly and bindingly in the member states and - unlike directives - does not entail transposition into national law. The regulation will apply from January 17, 2025.

18 Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending regulations (EC) NO 1060/2009, (EU) NO 648/2012, (EU) NO 600/2014, (EU) NO 909/2014 AND (EU) 2016/1011, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_41_2022_REV_1.

19 European Council Council of the European Union, Digital finance, https://www.consilium.europa.eu/en/policies/digital-finance/.

More Consumer Protection with the Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA)[20] is intended to increase the cybersecurity of products that are connected to each other or to the Internet. The products are manufactured by companies and sold to end customers, or they are used for production themselves or purchased as intermediate products. They can be installed or processed and are therefore also part of supply chains.

Scope

Under the planned regulation, manufacturers, producers[21], suppliers[22] and distributors[23] of products with digital elements[24] are to be held responsible. There are no size-related guideline values.

With a holistic approach, they will have to take care of the safety of their products from the conception or design and development phase, production, through placing on the market and use during the entire life cycle. They will be required to implement risk-appropriate measures. In addition to transparency for users, the European Union intends to ensure a coherent cybersecurity framework for hardware and software products. The CRA is not to apply to software provided as a service.

In the previous draft, products are categorized according to their criticality.[25] Thus, there will be non-critical, critical class 1 and class 2, and highly critical products with digital elements. As it stands, 90% of products fall into the first category (e.g., word processing products, photo processing products, smart speakers, hard drives, games). Class 1 critical products are expected to include password managers, network interfaces, firewalls, browsers and microcontrollers, and Class 2 operating systems, industrial firewalls, and CPUs. Highly critical products will likely include secure elements, hardware security modules (HSMs), secure crypto processors, and smart cards, smart card readers and tokens. Decisive for the classification are functionality, intended type of use (e.g. industrial control systems) and other criteria such as the extent of the impact of potential security problems.

Regulatory Requirements

For example, safety-related settings must be made for new products[26] and modules must be integrated into the product during development to protect the product ("security by default"). After the product has been placed on the market, the manufacturer must ensure the safety of the product for a maximum of 5 years, either through updates or by recalling the product and subsequently adapting it to the safety requirements. Manufacturers are required to carry out a comprehensive risk assessment, to anchor the identification of vulnerabilities in processes, to prepare technical documentation, including "software bill of materials",[27] and to report safety-relevant incidents to authorities and affected parties. The assessment of the fulfillment of the security requirements is carried out either by a self-assessment of the manufacturers or by a third-party assessment.

20 Proposal for a regulation of the European Parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF.

21 Article 10 Draft CRA.

22 Article 13 Draft CRA.

23 Article 14 Draft CRA.

24 Article 3 (3) Draft CRA.

25 Article 5 and Article 6 Draft CRA.

26 Article 10 draft CRA.

27 Article 23 Draft CRA.

Increased requirements for risk assessment processes apply to critical and highly critical products and goes up to require testing by independent third parties. Distributors and importers must ensure that imported products comply with the requirements of the CRA and that they are documented and labeled accordingly. Importers may themselves become manufacturers within the meaning of the CRA if they place a product on the market under their name or brand or significant adaptations.[28]

Violations of the CRA may result in fines of up to €15 million or 2.5% of global sales in the previous fiscal year.[29]

The assessment of the fulfillment of the safety requirements is carried out either by a self-assessment of the manufacturer or by a third-party assessment. Conformity is documented on the product with the "CE marking".

Member States must designate market surveillance authorities to be entrusted with the enforcement of compliance. They may order appropriate remedial action or product recalls.[30]

Implementation

The legislative process is currently underway. A first draft was published by the European Commission in September 2022. In May 2023, the draft was discussed in the European Council. The next step is the first reading of the draft regulation in the European Parliament. As a regulation, the CRA is directly applicable in the member states.

Critics and Comment

The European Union has increasingly focused on digital security with a number of regulatory projects, thus recognizing its significance and enormous importance in the course of the increasing digitization and networking of devices, facilities and processes.

Telos of Critical Infrastructure Guidelines Move Away from the Basic Idea of Security of Supply and Crisis Preparedness

The NIS-2 Directive and the CER both agree to create or expand minimum obligations for operators of critical infrastructure in order to minimize the risk of failure or disruption. The aim here is to maintain important social functions or economic activities in the internal market. Security of supply for society is only partially covered. The scope of application is considerably extended to the functioning of economic activities in the internal market. Along with this, the number of sectors will be increased. In the case of the CER, as a further development of the ECI Directive, this extension was necessary, since more sectors than just the energy and transport sector serve and secure the social functioning and economic activity. In the implementation and subsequent application of the NIS-2 Directive and the CER Directive, this means that many more operators of critical entities will have to comply with the requirements.

In Germany, it is currently assumed that around 29,000 companies and public entities will be subject to the NIS-2 Directive in the future. Previously, there were around 4,500 operators. In France, it is estimated that the number of companies and entities required to fulfil the requirements of NIS 2 will increase from currently 300 to 10,000. The amount of consulting work, especially for

28 Article 15 Draft CRA.
29 Article 53 Draft CRA.
30 Article 37 Draft CRA.

the many small and medium-sized companies, will increase enormously. Due to the shortage of skilled workers, also in the IT services sector, an enormous effort is likely to be required here to ensure proper implementation of the minimum obligations. Thus, there is a lack of resources in the operational area.
There is a risk of a considerable undermining of the original basic idea of establishing security of supply.

Two separate directives jeopardize consistency

The NIS-2 and CER Directives must be transposed into national law by the Member States and prescribe only a minimum harmonization framework. Member States may deviate from this while implementing both regulations. This leads to the fact that in the member states different far-reaching regulations are enacted in each case for the implementation of digital protection (NIS-2) as well as for physical protection (CER). For this reason, there is a risk of an inconsistent level of protection in the Union. In addition, both directives provide for the designation of a national reporting authority. Depending on the implementation, two different national reporting authorities could be designated for this purpose, as has also been envisaged in Germany to date.

In Germany, the Directives are implemented by different departments of the Federal Ministry of the Interior and Home Affairs. The NIS-2 Directive is implemented into national law in the Department for Cyber and Information Security, while the CER Directive is implemented in the Department for Crisis Management and Civil Protection. Accordingly, the risk of inconsistent implementation of both regulations cannot be dismissed. In France for instance the national cybersecurity agency *Agence nationale de la sécurité des systèmes d'information* (ANSSI), which is under the authority of the General Secretariat for Defence and National Security, is leading the work to transpose the NIS-2 Directive into French law in collaboration with government ministers. The General Secretariat for Defence and National Security is coordinating the implementation of the CER Directive, which means that different levels of authorities and departments are also responsible for its implementation.
The intended uniform level of protection in the Union threatens to become a patchwork quilt. Especially since overlapping responsibilities of authorities are to be expected.

DORA takes into account the importance of financial security

With DORA, the financial system is once again given special protection and its security is emphasized in comparison with other areas. Given the importance of a functioning financial system, this approach is undeniably correct and sensible.

CRA shifts responsibility for digital security to manufacturers, producers, suppliers and retailers

The CRA, with its basic idea of reducing the risk of security vulnerabilities in products with digital elements, is also a valuable measure for increasing the level of protection. At the same time, it shifts the responsibility for digital security away from consumers to manufacturers, producers, suppliers and retailers. It thus ensures a fairer distribution of the burden and a greater sense of responsibility for digital security among the obligated parties.

What's Next? Digital Security Can be Comprehensively Established through a Digital Resilience Law

However, to ensure a comprehensive and uniform level of protection, a regulation on European resilience is needed. The direct applicability of the regulation would create uniformity in the Union. The requirements of full harmonization could also prevent the patchwork already indicated above.

This regulation could take into account the sectors that are necessary for the nationwide provision of basic services to the population and should be prioritized according to their importance. Singling out individual sectors could probably be superfluous in the long term anyway, since the more extensive networking of products and facilities makes a separation by sector hardly seem possible anymore. Instead, the focus in the future should be on which subsectors and core areas of care require special protection.

Among other things, the increased attack surfaces, a multitude of professional actors and the threat of spill-over effects necessitate a change in the fundamental idea of protection and should direct the focus more toward reducing failures or disruptive damage, as well as quickly restoring functionality. Thus, the self-image of absolute damage prevention and full functionality is unlikely to be sustainable.

The regulation could also regulate and coordinate all areas of responsibility. It could encompass rights and obligations of users, manufacturers, producers, distributors, suppliers, operators, and state actors, and put the liability contributions of all actors in proportion. This regulation could also require only one national reporting authority, which could above all simplify cooperation among the member states and with the EU.

In addition to the cooperation of the national reporting authorities at the European level, the long-term goal should be a Europe-wide and comprehensive monitoring of the supply in order to detect failures or disruptions at an early stage and, if necessary, to be able to intercept them regionally, across countries in the European Union.

After all, digital security is a holistic task for society as a whole and requires a pan-European approach to security.

Recommendations for Cambodia

The experiences within the European Union in recent years can also be helpful for Cambodia's future developments in the area of digital security and allow some conclusions to be drawn.

Clearly assign responsibilities

First of all, it is crucial that there is a clear division of responsibilities. Ideally, an independent national authority should be responsible for digital security. This authority is responsible for coordination and consultation with the other departments involved in the creation of a cybersecurity strategy.

Create a Cybersecurity Strategy

The cyber security strategy must start with an analysis of the threat situation in cyber and information space. In addition to general geopolitical developments, it should also address regional characteristics and specific threats. The strategy must also contain clear objectives. The target formulations should be provided with a time frame for implementation. By defining interim targets, the timetables can also be adjusted on an ongoing basis. The overall implementation framework should not be longer than 5 years so as not to jeopardize the further updating of the strategy in line with developments. To achieve the objectives, the strategy must identify instruments and means with which the objectives are to be achieved. In addition, the means and objectives should be provided with financial resources for application and achievement.

In addition, all key players who bear responsibility for digital security must be included in the strategy. These include, above all, consumers, commercial enterprises (including along the supply chain) and

state institutions as customers, manufacturers, operators and product developers, the state as an actor, as well as politics, society and the media. The role of the actors should then be recorded. Based on these roles, there are different areas of responsibility and requirements for action that are crucial for digital security regulation.

Establish an independent national cybersecurity authority

A national and independent cybersecurity authority should be established (e. g. based on the model of the ANSSI in France). This should be implemented as a central reporting office for incidents as well as being entrusted with the implementation of the cybersecurity strategy and assuming a hinge function between the responsible ministerial authority and the cybersecurity stakeholders.

Regulating digital security

A uniform law to increase digital resilience is a considerable advantage, especially in the context of regulation. The roles defined in the strategy can be used to identify areas of responsibility for the stakeholders. The respective areas of responsibility can in turn be used to formulate various obligations and measures that describe the contribution of the respective actor to increasing resilience. Coordinated obligations and measures ensure a coherent national legal framework, which can also take the responsibility of product manufacturers and consumers into account to an even greater extent than legal regulations on digital security have done worldwide to date.

Supporting supra-regional cooperation and international initiatives

Participation in supra-regional cooperation and communities of interest is essential for international networking, building trust and partnerships. For Cambodia, it would make sense to push for greater cooperation in cyber security within the Association of Southeast Asian Nations (ASEAN). In addition to the exchange of information, this could also include joint exercises between the countries. Such training increases trust and ensures more intensive cooperation. Furthermore, joining the International Counter Ransomware Initiative would be worth considering for Cambodia. The aim of the now 50 member states is to cooperate in combating and prosecuting ransomware groups. The initiative aims to jointly build capacity and strengthen resilience.

Cybersecurity

Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law

Kaspar Rosager Ludvigsen

Abstract

Because digital devices and systems are widely used in all aspects of society, the risk of adversaries creating cyberattacks on a similar level remains high. As such, regulation of these aspects must follow – which is the domain of cybersecurity. Because this topic is worldwide, different jurisdictions should take inspiration from successful techniques elsewhere, with the European Union (EU) and the US being the most experienced and long-standing. What can be derived from their approaches separately to be used in other democratic jurisdictions, and what happens when we compare them with this pragmatic approach in mind? Cybersecurity is oddly enough quite well understood in most jurisdictions worldwide. However, concept comprehension cannot enforce or create compliance, hence the need for good regulatory approaches. The comparative legal analysis of the EU and the US show that there are large differences in definitions and enforcement, but some concepts are repeated in both jurisdictions. These can be further refined to become derivable principles, which can be used to inspire legislation in any democratic jurisdiction. They are: Voluntary Cooperation, Adaptable Definitions, Strong-arm Authorities, Mandated Computer Emergency Response Teams, and Effective Sanctions. These 5 principles are not exhaustive but combine classic regulatory and practical lessons from these two jurisdictions.

Introduction

Cybersecurity is the essential defence in digital systems, and is mandatory to prevent other people, government entities, machines, and others (collectively known as adversaries) to access, control, or destroy digital systems or devices. Cybersecurity can be negatively defined as a state of peace and lack of cyberattacks succeeding (Zdzikot 2022, 17–18). Some jurisdictions have extensive positively written and mandated legislation, which require cybersecurity from private and state actors, or which lets states supervise or support companies or individuals in attaining adequate cybersecurity, such as Poland (Brzostek 2022), Germany (Martini and Kemper 2022; Schallbruch and Skierka 2018) or the US (Lessambo 2023; Lubin 2023; Fischer 2013)”ISBN”:”978-3-031-23483-5”,”language”:”en”,”note”:”collection-title: Palgrave Macmillan Studies in Banking and Financial Institutions\nDOI: 10.1007/978-3-031-23484-2_5”,”page”:”57-78”,”publisher”:”Springer Nature Switzerland”,”publisher-place”:”Cham”,”source”:”DOI.org (Crossref. However, this is not the case everywhere, and those jurisdictions who lack the understanding or implementation of the regulation of cybersecurity is whom this paper is written for. Considering what existing legal systems have done, through comparative legal analysis, is the tool to seek inspiration for new legislation in any given country.

We therefore set out to give inspiration to the legal systems who have yet to take cybersecurity into their own hands and mandate the necessary technical requirements and powers to the right authorities. We do so through comparative legal analysis (this is also the methodology) of two large legal systems, the European Union (EU) and the US. These are large and influential legal systems globally and have regulated cybersecurity for many years. From this analysis, we derive 5 principles which could be used to design custom cybersecurity regulation in jurisdictions which lack them. These are: Voluntary Cooperation, Adaptable Definitions, Strong-arm Authorities, Mandated Computer Emergency Response Teams, and Effective Sanctions.

Cybersecurity Regulation in EU and US Law

Before making any recommendations, comparative legal analysis is necessary to show where other jurisdictions are regarding the regulation of cybersecurity. This consists of characterising

the systems and include references to the relevant legislation and policy,[1] which for both US and EU law is freely available online on websites hosted by both jurisdictions. We start with the EU.

EU

EU is not just one legal system; it sits above the jurisdictions of each of the 27 Member States (MS) and is therefore what we could call a "supranational" (Canihac 2020; Gabriel 2019) legal system.[2] The EU regulates cybersecurity in its product legislation, its separate specialised rules, critical infrastructure legislation, and indirectly in legal acts such as the GDPR.[3] The EU cannot legislate directly on areas such as cybercrime, or criminal elements of cybersecurity otherwise, as this is limited by the Treaty of the Functioning of the European Union, where the EU does not have sole or shared competence on the topic of criminal law,[4] which is required for it to legislate and regulate the area.

Specialised rules include the Cybersecurity Act (CA)[5] and the Cyber Solidarity Act (CSA),[6] while product legislation covers everything from e.g., those regulating Medical Devices, the Medical Device Regulation (MDR),[7] to the AI Act[8] and the Cyber Resilience Act (CRA).[9]

EU has cooperative mechanisms between big private cybersecurity providers (Bossong and Wagner 2017), or big structural companies such as Meta, which exist in practice, but will only be explicitly mentioned in the upcoming CSA. It has a central authority in the form of the European Union Agency for Cybersecurity (ENISA), empowered in the CA, though MS authorities play the largest role, meaning these are all relevant and important both currently and going forward. Critical Infrastructure includes the defences of all systems which are necessary for the functioning

1 Further in-depth comparative legal analysis is outside the scope of this paper, additional research by the author (Ludvigsen 2023; Ludvigsen and Nagaraja 2022b; 2022a)therefore, also increase. This paper uncovers how the cybersecurity of medical devices is currently regulated and how it can be improved going forward. First, the paper compares the regulation of medical device cybersecurity in the European Union, the United States and the United Kingdom (UK or others (van 't Schip 2024; Chiara 2023; Carr and Tanczer 2018; Casarosa 2022)develop and produce modern ICT products in a collaborative network: a supply chain. From a cybersecurity perspective, each actor brings new vulnerabilities for the entire chain and, in turn, the ICT product created by the chain. This problem should be addressed by supply chain cybersecurity, a type of cybersecurity policy that aims to prevent disruption of a supply chain's digital assets by internal or external actors. The EU Network and Information Systems (NIS2 should be consulted for this instead.

2 This refers to legal systems above others, which are not international or global, such as the African Union.

3 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) [2016] OJ L 1191

4 See Art 3 and 4 of the Treaty of the Functioning of the European Union.

5 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L151/15.

6 Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209 final, 2023/0109 (COD).

7 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L117/1.

8 REGULATION (EU) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 (Final Draft).

9 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, 2022/0272 (COD).

of any MS, meaning that NIS1[10] and NIS2[11] must be included. Sadly, the NIS1 implementation was considered to be fragmented and lacklustre (Ludvigsen, Nagaraja, and Daly 2022; Wallis and Johnson 2020; Kelemen, Szabo, and Vajdová 2018).

Cybersecurity in product legislation drives practical implementation across sectors and by private actors, who then must expect to be inspected or tested by relevant authorities, where security is usually regulated through guidance or indirect wording or interpretation of the primary product legislation like the MDR (Ludvigsen and Nagaraja 2022a; Biasin and Kamenjasevic 2020).[12] Or through all types of systems with network connectivity, which applies through the proposed CRA, meaning all products that provide such functionality much fulfil its minimum cybersecurity requirements across the EU (Eckhardt and Kotovskaia 2023). Cybersecurity matters in product liability situations too (Ludvigsen and Nagaraja 2022a), meaning the old and proposed new Product Liability Directive[13] will be used in situations where litigation is necessary, including security and safety (Buiten 2023, 22–23; Alheit 2001), as well as the proposed AI Liability Directive.[14]

US

US law is a wide concept, spanning both Federal law and State law (Hart 1954). We focus on the Federal rules, as making an overview of what each US state has implemented of legislation on top of the number of federal rules is beyond the scope of this paper.[15]

At this level, it exists past legislation which can be considered as cybersecurity regulation, such as the National Security Act of 1947,[16] and product legislation partially from the Consumer Product Safety Act.[17] Unlike EU law, US law excels in its specifications for the cybersecurity for the state as such, which can be seen with e.g., the Electronic Communications Privacy Act of 1986,[18] Economic Espionage Act,[19] Cybersecurity Act 2015[20] (CA2015), and recently, the policy of the National Cyber Strategy,[21] the Cyber Incident Reporting for Critical Infrastructure Act[22] and the Strengthening American Cybersecurity Act 2022.[23] The latter might not solve the fragmented state which some authors see the current cybersecurity landscape in the US being in (Kosseff 2018; 2023), and there is no equivalent all-encompassing general cybersecurity law in the US either yet (Lubin

10 Directive (EU) 2016/745 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L194/1.

11 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), [2022] OJ L333/80.

12 This should continue through mechanisms such as post-market surveillance (Badnjević et al. 2022; Zippel and Bohnet-Joschko 2017), where medical devices are a good example as well, even in a cybersecurity context.

13 Directive of the European Parliament and of the Council on liability for defective products, Brussels, 28.9.2022 COM(2022), 495 final, 2022/0302 (COD).

14 Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence
(AI Liability Directive)28.9.2022 COM(2022), 496 final 2022/0303 (COD).

15 The same can be said about the amount of specific legislation which exists in US law that regulates cybersecurity, for a good overview, see (Fischer 2013, 4).

16 Title 50, United States Code (U.S.C), Chapter 15, which is a barrier to sharing cybersecurity information if classified (Fischer 2013, 32). The U.S.C location denotes implementation into the Code.

17 U.S.C., Title 15, Chapter 47.

18 U.S.C., Title 18, Chapter 119, 121, 206.

19 U.S.C., Title 18, Chapter 90.

20 U.S.C., Title 6, Chapter 6.

21 https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/, last accessed 19 July 2024.

22 U.S.C., Title 6, Chapter 1.

23 Part of, the Consolidated Appropriations Act, 2022, see https://www.congress.gov/bill/117th-congress/house-bill/2471, last accessed 19 July 2024.

2023, 23). The potential in having strong connections between different authorities is great and considerable as well (Roesener, Bottolfson, and Fernandez 2014), creating synergies which are worth considering for other legal systems.

Products are further controlled by large central authorities in the form of the Federal Trade Commission (FTC) (Dibert 2016) and others, and there is privacy legislation like the Health Insurance Portability and Accountability Act (Jalali and Kaiser 2018) which involves some cybersecurity criteria. The role of guidance and choices in inspection will decide the cybersecurity level, but this can be a disadvantage as well (Roth 2014), something which is hopefully being changed over time in a security context.

Cooperation with private entities is natural and built into the CA15 (Kosseff 2018, 39), and exists informally as it does in the EU, and the power of other authorities, such as the Department of Homeland Security[24] (Ohm and Kim 2022) in relation to non-product cybersecurity regulation remains high as well. The nature of cybersecurity breaches (adversarial failures), however, in the form of private entities not wanting to share or release information until absolutely forced to, has consequences that warrant further scrutiny (Schwarcz, Wolff, and Woods 2022), and if this is continues to be an issue in US law, must be taken into consideration.

Because of the much more detailed legislation on criminal or unwanted cybersecurity actions, US law serves as a great example of state regulation of permissible security behaviour, such as in U.S.C., Title 6, Chapter 6. Combined with strong authorities, whose guidance and practice are clearly available,[25] makes for a somewhat different yet familiar approach to that of the EU.

Regulatory Mechanisms in Cybersecurity

There are many ways to potentially regulate an area such as cybersecurity. The following 5 recommendations are taken directly from both systems,[26] and should be used to consider how many jurisdictions, which does not yet have detailed legislation for cybersecurity, could design and make their own.[27] Initially, it must be said that extreme harshness or centralised control can impact innovation, willingness to corporate, or even make companies or individuals who create cybersecurity leave the country (Aggarwal and Reddie 2018; Huang and Li 2018; Lewis 2009). Great care must be taken to not cause worse side-effects from regulating cybersecurity, than leaving it unregulated.

Voluntary Cooperation

The relative power big companies hold within cybersecurity is very high (Farrand and Carrapico 2018; Carrapico and Farrand 2021; Moore 2010), as is the importance of communicating with providers of critical infrastructure and so on (Dykstra et al. 2022), even if partially state owned. Therefore, establishing both formal and informal communication paths are central to any kind of information sharing and control of the cybersecurity sphere, which is key to any kind of digital development.

24 E.g., https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing, last accessed 19 July 2024.

25 For example, the FDA publishes cybersecurity guidance for medical devices on its website, such as https://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act, last accessed 19 July 2024.

26 Each principle has references to where they are inspired from, but it is not always literally.

27 Such a system could be country like Cambodia, which this issue centres about. But the thoughts of this paper is applicable across the world.

An alternative option is to mandate certain threat indicators and defensive measures be shared to the government, which is required in US law.[28] This is very usable, since big corporations who have an interest in either being supported or assisted to update and patch vulnerable systems, can do so in a synchronous manner with the state. However, it can only be done well if there is little monetary or reputational risk to the private company providing this information, else it the information sharing may be illusory (Schwarcz, Wolff, and Woods 2022).

Inspiration can be taken from the CSA in EU law,[29] and especially from the CA15 in US law, and the focus should be on creating power within ministerial or state organs, who can facilitate the contact and maintain it, and integrate these communication channels into all types of state infrastructure – as cyberattacks can happen anywhere, from government computers, hospital equipment, or school iPads.

Adaptable Definitions

Technology changes over time, especially when it comes to software and hardware, meaning that the regulation of cybersecurity should be able to adapt in turn. This can be done in variety of ways, which could be so make the legislation very technology neutral (Reed 2007), which is seen in the proposed CRA from the EU, or in the amount of detailed technology specific legislation (Ohm 2010) there exists in the US related to cybersecurity .[30] A good middle ground could be to have legislation which is continuously improved, with sunset clauses which stipulate that the technology regulated is reviewed within a set time period. This could be beneficial when new techniques such as homomorphic or quantum encryption (Kop 2021) become widespread, or the use of Large Language Models increases in the cybersecurity area, or how we saw in practice that cybersecurity of cloud storage became as important as client-side server storage.

An example from US law, is its approach to how post-quantum cryptography will affect national security, and how systems can be migrated to post-quantum defendable systems:

> *... shall issue guidance on the migration of information technology to post-quantum cryptography, which shall include at a minimum-*
> *(A) a requirement for each agency to establish and maintain a current inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers, prioritized using the criteria described in subparagraph (B);*
> *(B) criteria to allow agencies to prioritize their inventory efforts; and*
> *(C) a description of the information required to be reported pursuant to subsection (b).”*[31]

In essence, how the cybersecurity regulation decides to define the technology and subjects it wants to cover should be written and practiced in a flexible manner, which may include adaptable definitions, or implicitly so, through technology-neutral terms.

Strong-arm Authorities

Within the cybersecurity community, there has long been a wish for authorities who both understand the nature of security (Abelson et al. 2015; Anderson and Moore 2006), but also provide sanctions for those who chose to disobey the rules. The latter can cause disruptions within various types of product manufacturers, as development costs are naturally lower if

28 U.S.C, Title 6, Chapter 6, §1504.

29 Inspiration can also be taken from individual Member States of the EU, but this is outside the scope of this paper, and varies significantly.

30 For an overview of the US situation, see Fischer (2013), though this lacks newer legislation.

31 U.S.C, Title 6, Chapter 6, §1526, part a, 1.

poor cybersecurity, or none, is chosen. Comprehending cybersecurity at a fundamental level is necessary because cybersecurity surrounds us and can cause accidents or failures which can harm individuals (Ludvigsen and Nagaraja 2022a), businesses (Alharbi et al. 2021), and entire nations,[32] or at a complete global scale.[33]

With how ENISA is empowered in the EU,[34] and how the FTC is supposed to be,[35] should serve as inspiration as to how to design such a mechanism in a home jurisdiction. An issue arises with those two, in the form of a lack of legal requirements for the professions and skills of staff.

A solution for this is found in the AI Act, which in Article 70(3), where requirements for staff are positively listed, states:

> *"Member States shall ensure that their national competent authorities are provided with adequate technical, financial and human resources, and with infrastructure to fulfil their tasks effectively under this Regulation. In particular, the national competent authorities shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of AI technologies, data and data computing, personal data protection, cybersecurity, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements. Member States shall assess and, if necessary, update competence and resource requirements referred to in this paragraph on an annual basis."*

Finally, tightly controlling and monitoring cybersecurity manufacturers and distributors too much can lead to a loss of trust, and thereby monetary or reputational losses for the state in question, and this aspect must be considered as well when designing the regulation.

Mandated Computer Emergency Response Teams

Writing about or announcing regulation of cybersecurity is not the same as committing to it in practice. To prevent attacks, create defences, and most important, maintain of all this, teams and large amounts of individuals must be at the disposal of the state in some practical manner. This is core part of both EU (CSA proposal) and US law,[36] and requires resources, available space for them in a branch of the government, and collaboration with companies and other actors who share critical information when an incident occurs.[37]

From the CSA, its purpose is worth showcasing, as it could be very useful for building national cybersecurity legislation for these types of response teams:

> *"This Regulation lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, in particular through the following actions:*
> *(a) the deployment of a pan-European infrastructure of Security Operations Centres*

32 For an Estonian view on this problem, see Ebers and Tupay (2023).

33 See the Crowdstrike Global Outage as an example, https://www.bbc.co.uk/news/articles/cp4wnrxqlewo, last accessed 19 July 2024.

34 Primarily use CA as inspiration, as ENISA only has sporadic mentions elsewhere. See the CA, Art 6, 7, and 8, for information about the general powers of the ENISA.

35 Criticism of the lack of enforcement by the FTC justifies focusing on what it should do, over what it does do (Schwarcz, Wolff, and Woods 2022, 45), should be considered.

36 As seen in the National Preparedness System (which includes cybersecurity related scenarios), U.S.C, Title 6, Chapter 2, §742. Worth noting that such emergency response teams also exist under U.S.C, Title 6, Chapter 6, §1522 and §1523, and but are mostly detailed in policy documents and the like, unlike what is detailed in EU's CSA.

37 Art 59(4) of the AI Act is also good as inspiration here.

> *('European Cyber Shield') to build and enhance common detection and situational awareness capabilities;*
> *(b) the creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, and immediate recovery from significant and large-scale cybersecurity incidents;*
> *(c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents."*[38]

These teams, or whatever structure is chosen, should have their own legal provisions, to ensure their availability and adequate skillsets, and exist both at a state and at a local level, akin to how Security Operation Centres[39] exist at an overarching level in the CSA, and National Security Operation Centres.[40]

Effective Sanctions

Preventing continuous breaches of cybersecurity, either by manufacturers, individuals or groups, or foreign states, requires the right answer (Rusinova and Martynova 2023). First, authorities who can inspect, withdraw, or ban products from a market are necessary.[41] Examples of these kinds of powers can be seen in e.g., the FTC or the FDA in US law, or authorities in the AI Act, CRA, CSA and so forth. Secondly, criminal provisions as well as the needed oversight must be considered as part of the regulation of cybersecurity.[42] As foreign states are strong adversaries, special measures, perhaps in relation to the military, should be considered, and represents international law more than domestic law, as it must be considered alongside the Laws of War. This is because cyberattacks can constitute Acts of War (Gervais 2011), and defending against such actions must be understood in this context, and prepared in the relevant legal system. While it can at times be difficult to decide on how, and why in an international legal context (Pomson 2023), it must be either be built into either legislation and/or policy documents.

Conclusion

In this paper, we have made a quick overview of how US and EU law regulates cybersecurity and formulated 5 principles inspired by elements from both legal systems. The principles have relevance for any state who has yet to make its own cybersecurity regulation and consider existing and functioning solutions, which can help guide countries like Cambodia or others who lack such laws.[43] They are not exhaustive but give an overview of the areas which must be considered. This could be product regulation, state cybersecurity, criminal and other types of liability, and contingency efforts (in case of war or serious adversarial attacks).

While these can inspire some aspects of the process of rulemaking, the rest should be filled in with the relevant legal culture and needs of the country. For further references, the academic papers and legal sources cited should be read, and relevant national stakeholders (private and state) should be included in the drafting processes.

38 CSA, Art 1(1).
39 CSA, Art 3.
40 CSA, Art 4.
41 Fines tend to not be enough, see the commentary by O'Malley (2009).
42 Strong inspiration for both misuse, fraud, and specialised cybersecurity criminal law problems, can be found in U.S.C, Title 18, §1030.
43 Some jurisdictions who may not have literal statutory law that concerns cybersecurity, may use existing security, telecommunication, or similar legislation as a replacement until specialised legal sources are created.

Cybersecurity

Criminal Liability of Legal Person in Cybercrime

Dr. Meas Bora

Abstract

Cybercrime is borderless and causes challenging in Cambodia in context of digitalization. Laws and regulations of Cambodia are in amess, and might be fulfilled by drafted law on cybercrime which will be expected to be broad and comprehensive.

In terms of legal person criminality, there are positive developments although with some weak points or unclarity, such as criterion and principles on which such a criminal liability is imposed. As matter of practice, loophole is evitable, and need to look into another practice or laws or treaties, such as Budapest Convention, helping legal construction in future by Cambodian courts.

Introduction

Intercommunication technology (ICT), includes computer, helps impart information, bringing social and economic prosperity to society; however, it might be used by offenders to offend community and cause insecurity as well. Computer crime/cybercrime is borderless.[1] There are several ways to deal with such an incidence through administrative, legal or judicial measure. For example, it is through adoption of law/statute on cybercrime in which there are criminalization of some acts and imposition of liability for breaching thereof.

For Cambodia, development of ICT crime is slowly in progress and with a few criminalized provisions starting from 2010 criminal code. As well, there is no academic paper addressing issue of criminal liability in cyber matter. It is a purpose of this paper to explore historical development of criminal liability since the code till current, drafted law on cybercrime (drafted law). It will take into account the foreign norms as bench mark for thinking to identify gaps in Cambodian laws related to criminal liability of legal persons for cybercrime with possible recommendations, if any, at the end of the paper. Before doing so, some relevant issues, such as cybercrimes will be highlighted.

Terminologies, Offense and Liability Under Foreign Laws

Some Terminologies

Legal framework contains piece of laws or whole law addressing cybercrime, cyber security and personal data protection together or separation of this each law[2]. Regardless of this, law contains offense, liability, defense, who are liable and so on.

First of all, we need to be aware of some key terminologies. **Service providers (SP)** are generally defined broadly to include access provider (internet company), searching, hyperlink, hosting and caching[3]. The last two are different in terms of permanent or temporary storing of data. **Data** refers to traffic data (computer one), fact, information or...**Computer system (cs)** refers one or more item together playing role in automatic process of data while device, like disk, which is a part of computer system. **Interference** is obstructing...which is different from intercepting data or computer system since, for intercepting, technical means are used to pursue intended act[4]. **Child** was defined a person under age of 18[5].

1 Libor Klimek, Criminal Liability of Legal Persons in Case of Computer Crime: A European Union Response, 15 (2) ICLR, 2015, pp. 135-143, p.141.

2 Cybercrime involves use of a computer or internet; Singapore has two separate laws (2017 Computer Misuse Act and 2018 Cybersecurity Act, see Asian Vision Institute (AVI), Kong Phallack et al., Cybersecurity Legislation in Cambodia: Policy to Improve Cyber Readiness and Resilience, (Issue 1, 2022) p. 5-6 (Cybersecurity Legislation in Cambodia).

3 Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime, 2013, s.3(3) (SADC Model Law).

4 ETS Convention on Cybercrime, 23.XI.2001, Article 1 (Budapest Convention); Commonwealth, Model Law on Computer and Computer Related Crime, s.8, 2017.

5 Budapest Convention, Article 9(3). For definitions are on electronic communication, hindering, hyperlink and device, see SADC Model Law, supra note 3, s. 3 (12 and 15).

Offenses

Cybercrime is defined as acts committed through computer system or using computer or internet; attacks are non-technical and focuses on human being, individual as victim. This makes distinction with cybersecurity crimes whose victims are government or infrastructure[6]. Computer or computer system is narrow meaning than electronics which might include other forms of communication, such as telephone[7].

Legal instrument classifies cybercrime into three types: relating confidentiality, integrity and availability of computer data and system (illegal access, illegal interception, data interference, system interference, misuse of devise[8]); computer-related offense (forgery, fraud, copyright and related rights) and content-related offence (child pornography).[9]

To illustrate, article 2 of the Budapest convention on Cybercrime (Budapest Convention) is quoted as a whole:

> ***Illegal access:*** *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

Illegal interception (II) is different from illegal access (IC), using technical means to intentionally transmit computer dada (CD), including electromagnetic emission from CS carrying CD[10]; it is not just accession to CS. Data interference (DI) is act of deletion or alteration of CD without right[11]. System Interference (SI) is different from DI since it needs to cause serious hindering of CS functioning via, for example, deleting data[12]. Lastly, Act of, for instance, producing a device[13] with intent to commit offense in article 2 to 5 is criminalized[14].

Forgery and fraud are computer-related offense. The former is act of alteration…resulting in inauthentic data for intentionally act for legal purpose as it is authentic one[15]; while the latter refers to act causing loss of property to another person by deletion of CD with fraudulent intent of procuring economic benefits for oneself or another person[16].

Article 9 of the Budapest Convention criminalizes act of producing…child pornography for the purpose for distribution through CS[17]. Lastly, copy right and related rights might be breached through CS and that needs to be criminalized. It covers acts infringing obligations under relevant convention, such as Bern Convention; it is committed on commercial scale willfully by means of CS[18].

6 Cybersecurity Legislation in Cambodia, supra note 2, p. 5.
7 Electronic communication means any transfer of signs, signals or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system, see SADC Model Law, supra note 3, s.3(11).
8 Device means broadly, including but not limited to keyboard, mouse…, id., s.3(10),
9 ETS 185, Cybercrime Convention, Explanatory Report (Explanatory Report), p.15.
10 Id., Article 3.
11 Id., Article 4
12 Id., article 5.
13 SADC Model Law, supra note 3, s.3(10).
14 Id., Article 6 (article 2 on illegal access; article 3 on illegal interception; article 4 on data interference; article 5 on system interference), explanatory report, supra note 9.
15 Id., article 7.
16 Id, article 8.
17 It is defined child and child pornography as well. It suggests not to lower than 16 age for criminal liability.
18 Explanatory report, supra note 9, Article 10, p. 17.

Criminal Liabilities of Legal Person

Generally, offenses are intentional offense covering general and specific-intent offense[19] or negligent[20]. Moreover, it is suggested to provide attempt to those offense for the matter of liability[21].

Term "without right" is general as defense for not being liable for physical person[22]. For example, if access authorized by authority, there is not criminal liability.[23] Act with lawful excuse or justification is not offending[24]. For some specific offence, child pornography, bona fide used child porn for scientific research...is a defense[25]. There is no general obligation on ISP to monitor data which stores; access, hosting, provider, hyperlinks and search engine providers are not liable, except, for example, the case of caching provider, the provider modified information....[26] For misuse of device, it will not be offense if not for commission or for authorized testing CS[27]. They might not be crimes if there are other means of addressing violations by providing effective remedy to victims of copy rights violation and doing as such does not derogate from obligation of State[28].

Both physical and legal person is liable. Liability of legal person does not relieve one of individual[29]. Official acts lead to legal person liability which needs to meet four criteria: 1. acts of officials (not simple employee) 2. in her or his capacity, 3. benefit for company...[30] Furthermore, official will be liable for act of employee under their control if he/she failed to supervise employee or agent who committed offense and for benefit of that legal person[31].

For legal person, liability is in case of being not compliance with order or decisions of authorities. There might be also civil and administrative liability in addition to criminal one[32]. Sentencing imposing principle includes effectiveness, proportionality and dissuasion.[33]

19 Budapest Convention, supra note 4, articles 2 and 3; not intent but only knowledge that acts will cause unauthorized modification of the computer content, see Nazura Abdul Manap, Alignment of Malaysia and ASEAN Agreements on ICT Law: A Review, 2(s)1, Brawijaya Law Journal, 2015, p.12.

20 Commonwealth Model Law, supra note 4, s. 9 (illegal device).

21 Explanatory Report, supra note 9, p.19 on Article 11.

22 Explanatory Report, supra note 9, Article 12, p.20.

23 Id., Article 2, p.9.

24 Commonwealth Model Law, supra note 4, s.5, 2017.

25 Id., s.10(2); SADC Model Law, supra note 3, s.13(2).

26 SADC Model law, id., s.36.

27 Budapest Convention, supra note 4, Article 6

28 Id., Article 10.

29 Explanatory Report, supra note 9, Article 12, p.20.

30 Id., Article 12, p.20.

31 Id., p.19 on Article 12, p.20; The Directive 2013/40/EU on attacks against information systems, Article 10(2). Article 12 of Budapest Convention – Corporate liability: *1* Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on*: a* power of representation of the legal person*; b* an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person*. 2* In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. *3* Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative*. 4* Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

32 Budapest Convention, supra note 4, Article 12.

33 Id., Article 13(1).

Offense and Liability under Cambodian Laws

Offenses

Till now, there are many pieces of laws directly or indirectly related to cybercrime. Those pieces of relevant laws are law on suppression of human trafficking and sexual exploitation (2008), law on copy rights and related rights (2003), law on post and telecommunication (2002), law on protection of patents (2001), law on geographical indications (2014), criminal code (2010), law on consumer protection (2019) and law on electronic commerce (2019). It is noted that Cambodia adopted separate law approach. The most relevant law dealing with cybercrime has been drafted by Ministry of Interior; while drafted law on cybersecurity and one on personal data protection have been drafted by Ministry of Post and Telecommunication. This section only focuses on cybercrime. It will present offenses in Cambodian laws which might be committed through CS following three types of sub-offense as mentioned above in section II.

Offenses Relating Confidentiality, Integrity and Availability of Computer Data and System

Starting from 1993 Constitution to drafted law in 2024, the constitution provides that secrecy of correspondence via ICT shall be guaranteed[34]. Criminal code criminalizes act affecting secrecy of telephone conversation[35]; act fraudulently accessing or remaining in data automate system shall be imprisoned from 1 month to 1 year and fine up to 2 million riels, sentence would be increased to 2-year imprisonment and fine of 4 million riels if such an act deleting or modifying data or causing damage to the system[36]. Article 429 makes a slight difference and it is independent offense. It prohibits act of modification, inserting or deleting in direct manner and fraudulently, of data into automated data processing system. Finally, it is an obstructing act of automated data processing system[37].

Articles 445- 448 of criminal code cover computer data; act giving data to foreign State faces criminal penalty, and obtaining information from foreign agent which might cause risk to national defense, shall be sanctioned with 7 years to 15 years in prison. In spite of this, these offenses are not through CS ones.

The law on e-commerce is much relevant to computer means offending, such as forging using ICT means[38], failure to follow duty to protect data[39], abuse of code[40], transactions by means ICT[41], and electronic instrument[42]. There are other criminal acts.[43]

Relevance to Computer-Related Offense

In 2002, Cambodian National Assembly adopted law on copy rights, and trade mark. This law criminalizes act of production…through broadcasting booth, change of information by means

34 Constitution 1993, Article 40(2).
35 Criminal Code 2010, Article 318.
36 Id., Article 427.
37 Id., Article 428; - a system of one or more computers and associated software with common storage, available at Automatic data processing system - definition of automatic data processing system by The Free Dictionary (accessed on 24 August 2023).
38 Law on E-commerce 2019, article 59.
39 Id., article 60.
40 Id., article 62.
41 Id., article 63.
42 Id., article 64.
43 Id., articles 35, 55-64.

of electronics[44], and imposes criminal sanctions in case of breaching[45].Criminal code sets forth acts of fraud[46] and related offense, such as breach of trust[47], dishonesty[48]; however, they are not cybercrimes.

The law on protection of consumer contains a few provisions on criminal liability and physical acting crime (unfair practice, pyramid sale scheme and failure to provide minimum information for consumer)[49].

Content-related Offense

Law on suppression on human trafficking in 1996 and amended in 2008 prohibits many acts, including child porn although only two articles and they are only physical offending act[50]; Likewise, it is the Criminal code 2010. It proscribes act of pornography and other relevant acts; It is noted that it criminalizes act of participation of minor in sexual demonstration[51]. However, they are offense not through ICT[52]. Interestingly, drafted law on child protection (2023) who one of drafters is the author of this paper included ICT related content offense, such as prohibition of online dissemination of porn[53], online grooming[54], online sexual extortion.[55] To illustrate, article 124 on prohibition of online and offline acts, is quoted:

> *1. It shall be prohibited to -*
> *a. produce, possess, offer, distribute, disseminate, import, export, interact with, access, and produce or disseminate material to advertise child sexual abuse material, including live-streaming of child sexual abuse.*
> *b. Knowingly possess child sexual abuse materials, including electronic child sexual abuse materials, regardless of whether there is an intention to distribute.*
> *c. Attempt or to aid or abet the commission of an offence under article 124 of this Law.*
> *2. For whatever reason, any presumed consent by a child under the age of eighteen (18) shall be null and void.*

Offenses under Drafted Law on Cybercrime

Drafted law has been initiated long time ago, and now it almost comes to finalization stage. The author expects that much content would remain. Following the law formality, the draft contains article 3 on 19 terminology of which is much detailed if compare with Budapest Convention. Among them are offenses: computer data storage medium, cryptocurrency.

There are 23 offenses in the drafted laws classified more than three types, might be committed through computer system:

44 Law on Copy Rights 2003, Article 62.
45 Id., article 64 and 65.
46 Criminal Code, supra note 35, Article 377.
47 Id., Article 391.
48 Id., Article 384.
49 Law on protection of consumer 2019, Article 44-45, 48,
50 Law on Suppression of human traffic (2008), Articles 39 -40.
51 Criminal Code, supra note 35, Article 346.
52 Id., article 341 (indecent act upon minor under 15 age old), article 246 (sexual transgression), article 249 (sexual organ exposure), article 250 (sexual harassment),
53 Drafted Law on Protection of Children (Drafted Law on PC) (23 June 2023), Article 124.
54 Id., Article 127
55 Id., Article 128.

Integrity of CS: distribution of data illegally by competent authority, article 25; nonfulfillment of duty to maintain computer data, article 30; illegal access, article 33; abuse of permission to use CS, article 34; data espionage, article 35; act of damaging computer data, article 37; act of damaging CS, article 38; misuse of device, Article 36.

Computer related offenses: provision of false information by service provider, article 32; fraud through computer system, article 43; forging via computer system, article 44; forging individual identification, Article 45; provision of false information, article 46.

Content related offenses: pornography, article 39; child sexual exploitation, article 40; abuse or threat by means of ICT, article 41; violation of copy rights, article 42 and

Other offenses: failure in management of consumer registration, article 24; negligence by competent authority, article 26; uncooperative act to enforcement official, article 27; breach of confidentiality, article 28; breach of confidentiality of summon, article 29; cryptocurrency, article 31.

Criminal Liability of Legal Person, Defense and Sentence

In General

Criminal code classified three types of offense[56] in broad fields[57], might be committed negligently or with intent (intent offense)[58]. Individual offender might be liable as principal or accomplice[59] or attempt[60]. He or she might be exempted from criminal liability if, for example, she or he was insane during the time of crime commission[61].

Individual, as official of company-legal person, is also liable separately from legal person he or she attached[62]. It is unclear what types of defenses applicable to individual also apply to legal person. Criminal code provides two types of sentences: principal and additional one. The former includes imprisonment and fine[63]. Legal person faces only fine as principal sentence[64], and other additional sentences[65]. According to the principle of legality, sentence shall be set forth in laws and need to be pronounced by judge in order to be enforceable.

Besides the general rules, liability, defense and sentence were mentioned in specific laws which are applicable. For example, law on suppression of human trafficking provides criminal prosecution exemption for child under 15 ages old committed sex intercourse with under 15 age child (article 42) and indecent act upon under 15 age old child.[66]

Related to Cybercrimes

All three types of acts mentioned in Criminal Code might be committed by a group of persons or in conspiracy. Participating in such a group shall be sentenced from 1 year to two years and fine

56 Criminal Code, supra note 35, Articles 46-48.
57 Offenses against human, property....
58 Id., article 4.
59 Id., Article 29.
60 Id., article 27.
61 Id., Article 31.
62 Id., article 42.
63 Id., Article 43.
64 Id., article 167.
65 Id., article 168.
66 Law on Suppression of Human Trafficking, supra note 50, article 44.

up to 4 million riels[67]. All act might be attempted and face similar penalties. Article 432 provides additional sentence; among of them, restriction of civil right is one option. It is noted that legal person is not liable for offense. Likewise, it is not clear if excuse or justification might be resorted to by accused charged of the offenses in this section. Law on e-commerce imposes criminal liability upon legal person as well[68].

Law on e-commerce impose criminal liability for legal person for 8 offenses (article 65), including forging code-sending virus transferring code (article 59). Fine is double and with any of additional sentences.

Drafted law on child protection imposes sanction upon individual, including legal person failing to follow warning or instruction by Ministry of Post and Telecommunication[69], sharing of own personal sexual image of under 15 age old between them is not crime[70]. Furthermore, accused age of more than 5 years (19 years old) than 15 child age old (victim) might be exempted from criminal liability if he/she fulfils three conditions, one of which is consent[71].

Article 47 and 48 of drafted law on cybercrimes provide attempt and accomplice respectively for cybercrime in articles 24-46. Accomplice here refers to act of joining group or conspiracy created to commit those cybercrimes. Accomplice is similarly sanctioned. Participation in group or in conspiracy will be exempted from sentence if, before accusation, such a person pointing out group or conspiracy to competent authority and leading known of identity of other members. This might be considered as a part of excuse or justification in addition to the fact that any person acting legally or legally permitted which is considered as not criminal[72].

Legal person is also criminal liability separate from individual one[73]. Legal person is liable according to article 42 of Criminal Code. It bears as well additional sentence according to Article 168 of Criminal Code[74].

Sanction covers provisional fine[75] administrative or criminal one[76]. It depends on gravity of offense, and if so, both fine and imprisonment were provided[77]. Some offense contains only fine[78]. Generally, fine for physical person offender is higher than one for legal person. For example, breaching confidentiality, fine of 20 million riels is imposed for physical person, but 500 million riels for legal person[79]. Maximum of 10 year imprisonment is for illegal access to data related to

67 Criminal Code, supra note 35, Article 430.

68 Law on E-commerce, supra note 38, Article 65; Law on geographical mark contains a few articles on crime and liability for legal person as well; however, they did not have any relevance to computer means of commission (Law on Geographical Mark 2001, articles 38-40).

69 Drafted Law on PC, supra note 56, article 123.

70 Id., article 125.

71 Id., article 127 (4).

72 Drafted Law on Cybercrime, Article 25.

73 Id., Article 23.

74 Drafted Law on Cybercrime, supra note 72, Article 23. Legal person is liable for offenses acting breach article 24 (failure in management of consumer registration), article 28 (breaching of confidentiality), Article 29 (breaching of confidentiality of summon), article 30 (nonfulfillment of duty to maintain computer data), article 31 (advertisement of cryptocurrency), article 32 (provision of false information by service provider), article 36 (misuse of devise), article 37 (act of damaging computer data), article 38 (act of damaging computer system), article 42 (violation of copy rights), article 43 (fraud through computer system), article 46 (providing false information).

75 Id., article 21.

76 Id., article 21.

77 Id., article 28.

78 Id., article 26.

79 Id., article 28.

national security.[80] 5 year imprisonment maximum (misdemeanor) is for an offence for which legal person is criminal liability.[81] In this respect, legal person will not be liable for an attempted cybercrimes.

Analysis of Legal Person Criminal Liability

Drafted law criminalized more acts and details if compared with what mentioned in articles of Criminal Code and those in Budapest Convention which straightly only dealt with cybercrime, by adding new offense, such as giving false information by service providers, and extent relevance to cybersecurity (article 33), it covers as well procedure abuse offense. Subject of offense are officials. These different offenses emphasized means of commission-that is through ICT. Among of majority, less offenses are omissive.

Access to CS is broader in terms of types of computer data. Beyond the access, it is an access to use CS by copying and/or transfer of CD without permission, access by violation of security norm, access to CS carrying confidential date or related to national security. Difference from access, data interception shares similar content of Article 3 of the Budapest Convention. This is likewise act of devise misuse/illegal device.

For an access, content of article 427 of Criminal Code is similar to article 33 of drafted law except penalty thereof latter is heavier than. Article 428 and 429 of Criminal Code contain some elements in article 37 and 38 of the drafted law. This is matter of applicable law in case of liability arising. Lex generis/lex specialis, lex posterior/lex priori and principle of legality will play roles in construction and application of relevant provisions.

Difference from Budapest Convention, drafted law provides more grounds for exemption from criminal liability, such as with permission, without appropriate or right reasons, without legal permission in addition to lack of intent. There are inherent grounds mentioned in some offenses. Thus, it is beyond Budapest Convention which mentioned only “intention” and “without rights”. Terms “with permission, without appropriate or right reasons, without legal permission” are unclear. For bona fide scientific research might mean “right reason” defense for not breaching child pornography.

Review of relevant laws related to cybercrime or on cybercrime (drafted law), in terms of legal person criminal liability, nothing much than what mentioned in article 42 and 168 of the criminal code. Liability exists only there is law mentioning. Liability of legal person does not relief an individual from the same liable acts. Legal person faces only fine as a principal sentence in addition to additional sentences might be imposed by the courts (article 24).

Drafted law imposes liability for legal persons for 12 offenses[82], including breaching copy right (article 42), fraud through computer system (article 43). Fine, as principal sentence, is higher than one for individual offender (article 42), for example. Liable person shall be representative or organ of legal person; thus, act of normal employee, except he is a representative, does not lead to legal person liability. This is narrower than Budapest Convention which impose liability of legal person whose employee under supervision of representative thereof committed offense for benefit of legal person or the representative failed to supervise employee.

Budapest Convention adds more criterion for liability; that is commission of offense in her or

80 Id., article 33.
81 Id., article 46.
82 See supra note 74.

her capacity as representative of legal person. This does not find in article 23 of drafted law. Finally, effectiveness, proportionality and dissuasion -guiding principles for imposing liability and sentence- are not mentioned in the drafted law.

Article 49 exempts individual from liability if he or she revealed members of group to authority. This might not relief legal person from liability.

Conclusion and Recommendation

Review of legal development related cybercrime chronologically reveals from pieces of laws to current drafted law on cybercrime in terms of crimes, liability and sentence that they are detailed and broad. However, in terms of legal person liability for cybercrime, criterion for imposing liability is not clear, as well as principles for such imposition. Individual causing legal person liability is also narrow.

Changes to substance of provision on criminal liability of legal person, beyond the relevant one of criminal code, and to follow relevant substance in Budapest Convention is needed if full effectiveness of cybercrime law enforcement is wanted, by broadening types of persons attributed to legal person.

KONRAD-ADENAUER-STIFTUNG, CAMBODIA

House No 4, Street 462, Khan Chamkar Mon,
P.O.Box 944, Phnom Penh, Kingdom of Cambodia,
Telephone : +855 23 966 171
Email : Office.PhnomPenh@kas.de
Website : www.kas.de/cambodia
Facebook : www.facebook.com/kaskambodscha

9 789924 571254