

LEGAL MEASURES ON PERSONAL DATA BREACH IN THAILAND

BY

KORNWAT KAEWKULAYA

A dissertation submitted in fulfillment of the requirement
for the degree Master of Comparatives Laws

Ahmad Ibrahim Kulliyah of Laws
International Islamic University Malaysia

MARCH 2025

ABSTRACT

In recent years, Thailand has confronted an escalating risk of personal data breaches, which persistently impact cyberspace, with intense ramifications of identity theft. The root reason for this is a substantial breach of personal data, resulting in considerable harm to individuals and the loss of numerous valuable possessions. This cybercrime has evolved into both a national and global concern. This doctrinal research analyses the characteristics and operational categorisations of personal data breaches based in Thailand, emphasising current legal frameworks established to encounter these threats. The research continues to examine personal data breaches through the perspective of Islamic criminal law, providing an analysis of selected legal principles and approaches to this matter. Furthermore, this doctrinal research analyses Thailand's Personal Data Protection Act (PDPA) 2019 and the European Union General Data Protection Regulation (EUGDPR). The benchmark study illustrates how Thailand has effectively integrated and modified the EUGDPR's legal provisions inside its domestic framework. Besides, this research also explores the future direction of Artificial Intelligence's (AI) role in personal data breaches. The research finds that extensive legal frameworks, particularly the PDPA and the Cybersecurity Act 2019 (CSA), are already established alongside overarching legal principles derived from Thailand's comprehensive legal system. Meanwhile, the Computer Crimes Act 2017 (CCA) has a positive effect from the specifically mentioned amendments that enhance the legal countermeasures against illegal access offences. The research findings show that Thailand's achievements in mitigating cyber dangers are praiseworthy. This research suggests additional legislation reforms and improved regional collaborations to maintain sustained efficacy.

خلاصة البحث

في السنوات الأخيرة، واجهت تايلاند خطرًا متزايدًا لانتهاكات البيانات الشخصية، التي تستمر في التأثير على الفضاء الإلكتروني، مع عواقب وخيمة مثل سرقة الهوية. يعود السبب الرئيسي لذلك إلى الاختراق الكبير للبيانات الشخصية، مما تسبب في أضرار كبيرة للأفراد وفقدان العديد من الممتلكات الثمينة. لقد تطورت هذه الجريمة الإلكترونية لتصبح مصدر قلق على المستويين الوطني والعالمي. تقوم هذه الدراسة النظرية بتحليل خصائص وتصنيفات العمليات المتعلقة بانتهاكات البيانات الشخصية في سياق تايلاند، مع التركيز على الأطر القانونية الحالية التي تم إنشاؤها لمواجهة هذه التهديدات. كما تواصل الدراسة استكشاف انتهاكات البيانات الشخصية من منظور القانون الجنائي الإسلامي، من خلال تقديم تحليل لبعض المبادئ القانونية والنهج المختارة لمعالجة هذه القضية. علاوة على ذلك، تقوم هذه الدراسة النظرية بتحليل قانون حماية البيانات الشخصية في تايلاند (PDPA) لعام 2019 ولوائح حماية البيانات العامة في الاتحاد الأوروبي (EUGDPR). توضح الدراسة المرجعية كيف قامت تايلاند بدمج وتعديل الأحكام القانونية لـ EUGDPR داخل إطارها المحلي بشكل فعال. بالإضافة إلى ذلك، تستكشف هذه الدراسة الاتجاه المستقبلي لدور الذكاء الاصطناعي (AI) في انتهاكات البيانات الشخصية. تجد الدراسة أن الأطر القانونية الشاملة، لا سيما قانون حماية البيانات الشخصية (PDPA 2019) وقانون الأمن السيبراني (CSA 2019)، قد أسست بالفعل جنبًا إلى جنب مع المبادئ القانونية العامة المستمدة من النظام القانوني الشامل في تايلاند. في الوقت نفسه، لقانون جرائم الكمبيوتر (CCA 2017) تأثير إيجابي من التعديلات المحددة المذكورة التي تعزز التدابير القانونية لمواجهة جرائم الوصول غير القانونية. تُظهر نتائج البحث أن إنجازات تايلاند في التخفيف من مخاطر الفضاء السيبراني جديرة بالثناء. كما تقترح هذه الدراسة إجراء إصلاحات تشريعية إضافية وتعزيز التعاون الإقليمي للحفاظ على الفعالية المستدامة.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Comparatives Laws

.....
Sonny Zulhuda
Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Comparatives Laws

.....
Name
Examiner

.....
Name
Examiner

This dissertation was submitted to the Department of and is accepted as a fulfilment of the requirement for the degree of Master of Comparatives Laws

.....

Name

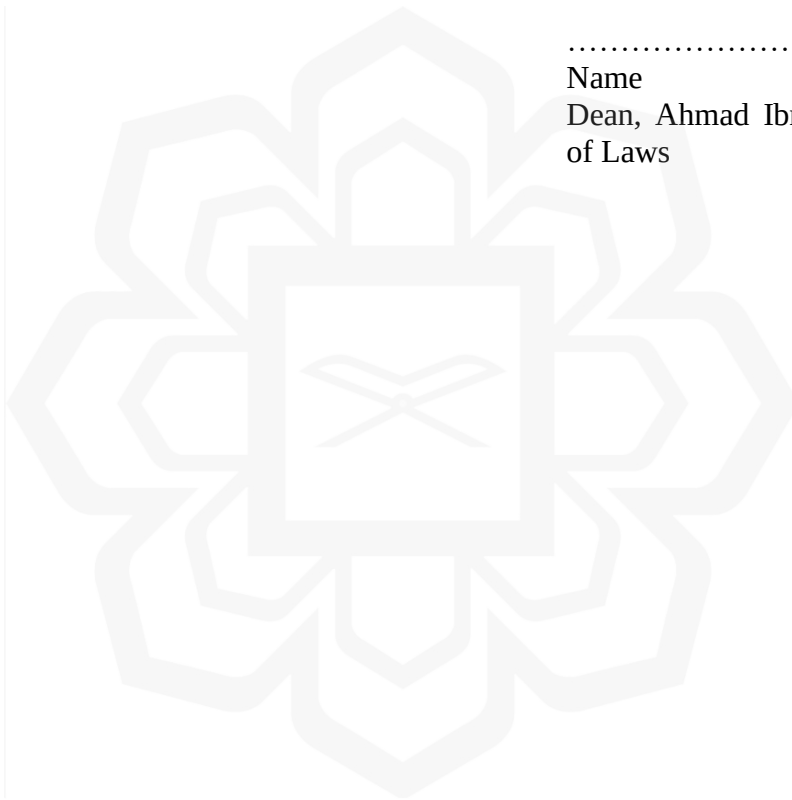
Head, Department of

This dissertation was submitted to the Ahmad Ibrahim Kulliyah of Laws and is accepted as a fulfillment of the requirement for the degree of Master of Comparatives Laws

.....

Name

Dean, Ahmad Ibrahim Kulliyah
of Laws



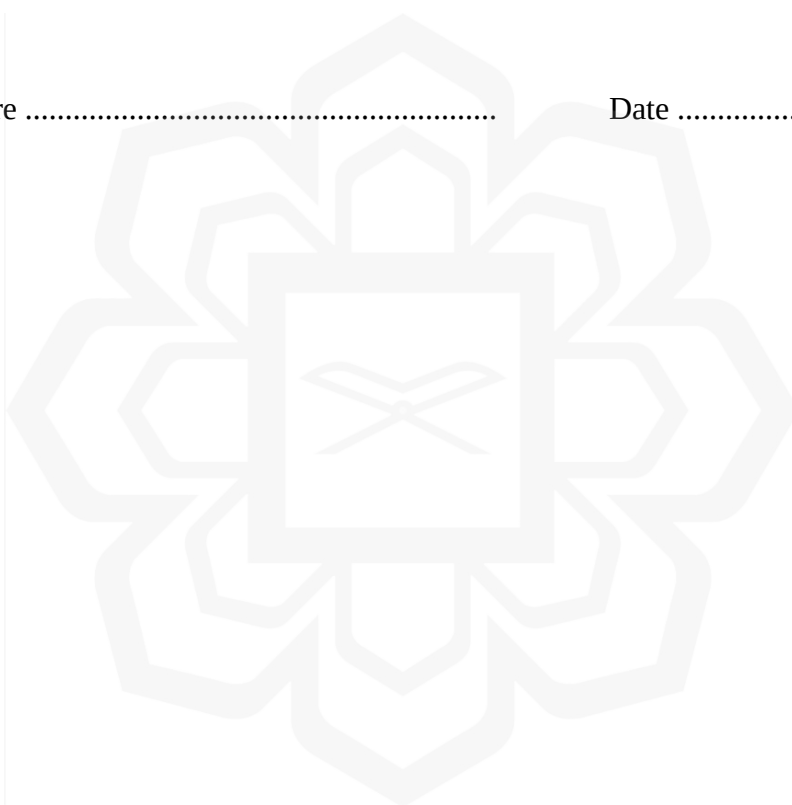
DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Kornwat Kaewkulaya

Signature

Date



INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF
FAIR USE OF UNPUBLISHED RESEARCH**

**LEGAL MEASURES ON PERSONAL DATA BREACH IN
THAILAND**

I declare that the copyright holders of this dissertation are jointly owned by the student and IIUM.

Copyright © 2024 Kornwat Kaewkulaya and International Islamic University Malaysia. All rights reserved.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.
2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.
3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Kornwat Kaewkulaya

.....
Signature

.....
Date

ACKNOWLEDGEMENTS

I would like to thank my parents and sister, who have dedicated and supported me in every decision-making process since I began studying at IIUM until this achievement. It is valuable to give this research as one successful to them. Secondly, for Assoc.Prof.Dr. Sonny Zulhuda, my supervisor because of his dedication to developing this dissertation and my performance, skills, and knowledge to understand and express it, also completed this dissertation. Thirdly, my beloved friends, as the first Thai students who have been my classmates since my bachelor's degree, especially Mr. Weeraphot Talordsuk, Mr. Keittisak Punkeaw, and Ms. Appassara Suwannaprasert. As they always send the initial assistance at the necessary time. Likewise, Mr.Sukrit Kimkleawkarn, Mr.Aoafa Haree, and Mr. Areef Hayeehasa, my Thailand IIUM students' friends, even though they studied in different Kuliyah, always stayed beside and supported me in every obstruction that came through. Significantly, I would like to send thanks and best regards to all Thailand's Legal practitioners who sent the warm welcome and excellent coordination to grant permission to interview both officially and unofficially from both private and government sectors. Especially the practitioners from PDPC, NCSA Thailand, and Digital Business Consultant Group Co Ltd. Without your opinions on the in-depth critiques on the crucial issue, this dissertation could not have been successful.



TABLE OF CONTENTS

Abstract	ii
Abstract in Arabic	iii
Approval Page.....	iv
Declaration.....	vi
Copyright Page.....	vii
Acknowledgements.....	viii
Table of Contents.....	ix
List of Tables	xi
List of Cases.....	xii
List of Statutes	xiii
List of Abbreviations	xiv
 CHAPTER ONE: INTRODUCTION	 1
1.1 Background of the Study	1
1.1.1 Thailand's Personal Data Breach Situation	3
1.1.2 Brief Thailand's History of Legal Framework development in Personal Data Breach Crime.....	7
1.2 Problem Statement.....	10
1.3 Research Objective	13
1.4 Research Questions.....	13
1.5 Literature Review	14
1.5.1 Nature and scope of personal data breach.....	14
1.5.2 Legal Measures on Personal Data Breach in Thailand	19
1.6 Research Methodology	24
1.7 Scope and Limitation of Study	25
1.8 Chapterisation.....	27
1.9 Significance of the Study.....	29
 CHAPTER TWO: PERSONAL DATA BREACH: NATURE, DEVELOPMENT, AND THE LEGAL ISSUES IN ISLAMIC CRIMINAL LAW PERSPECTIVE	 30
2.1 Introduction.....	30
2.1.1 Recent Case of Personal Data Breach in Thailand	31
2.2 The Nature of Personal Data Breach: Factors and Manners.....	37
2.2.1 External Operation	38
2.2.2 Internal Operation (Insider Threat).....	42
2.2.3 The Threat of Personal Data Security and Non-Malicious Incidents.....	43
2.3 Personal Data Breach under the Islamic Criminal Law Perspective	46
2.3.1 Information Security Perspective between Islam and Buddhist Faith	47
2.3.2 Current status of interpretation direction in ICL Perspective	52
2.4 Conclusion	60

CHAPTER THREE: ANALYSIS OF THAILAND'S LEGAL FRAMEWORK ON PERSONAL DATA BREACH.....	63
3.1 Introduction.....	63
3.2 Penal Code	70
3.3 Civil and Commercial Code	76
3.4 Computer Crimes Act 2007.....	83
3.5 Cybersecurity Act 2019	91
3.6 Thailand's Personal Data Protection Act 2019	97
3.6.1 Data Subject Rights.....	100
3.6.2 Data Controller Compliance	101
3.6.3 Civil Liability	106
3.6.4 Criminal Liability.....	109
3.6.5 Administrative Liability.....	110
3.6.6 The milestone incident: JIB Computer	111
3.7 Conclusion	114
 CHAPTER FOUR: THE LEGISLATION BENCHMARK ANALYSIS AND THE FUTURE DIRECTIONS OF PERSONAL DATA BREACH LAW	 116
4.1 Introduction.....	116
4.1.1 Thailand Legal Implementation Issues Analysis	117
4.1.2 The legal issues on Thailand's Personal Data Protection Act and Cybersecurity Act implementation	118
4.1.3 The Legal issues on the lack of procedure under administrative court dealing with Data Breach appeal and the special court division.....	122
4.1.4 Non- Effectiveness of the legal provisions regarding personal data breach	124
4.2 The Benchmarking Analysis: European Union General Data Protection Regulation and Thailand's Personal Data Protection Act	128
4.3 The Role of Artificial Intelligence in the Personal Data Breach	140
4.4 Conclusion	146
 CHAPTER FIVE: CONCLUSION AND RECOMMENDATION.....	 149
5.1 Conclusion.....	152
5.2 Recommendation and Suggestion	164
 REFERENCES.....	 167
 APPENDIX I: THE SUMMARY REPORT OF THE INTERVIEW WITH VARIOUS RESOURCES FROM THAILAND SUBJECT MATTER EXPERTS	 176

LIST OF TABLES

Table 3.1	The Summarisation of Thailand’s Legal Measures in The Event of a Personal Data Breach (The Substantive Legislation Only)	67
Table 4.1	The Benchmarking Analysis Between Thailand’s Personal Data Protection Act 2019 and the European Union General Data Protection Regulation 2016 in the Personal Data Breach event on the legal arrangements	129



LIST OF CASES

Thailand's Case:

- Decision of the Supreme Court of Thailand number 214/2498 (1955), Assistant Judges of the Supreme Court, 1st January 1970
- Decision of the Supreme Court of Thailand number 887/2501 (1958), Assistant Judges of the Supreme Court, 1st January 1970
- Decision of the Supreme Court of Thailand number 789/2502 (1959), Assistant Judges of the Supreme Court, 1st January 1970
- Decision of the Supreme Court of Thailand number 256/2516 (1973), Assistant Judges of the Supreme Court, 1st January 1974
- Decision of the Supreme Court of Thailand number 253/2520 (1977), Assistant Judges of the Supreme Court, 1st January 1978
- Decision of the Supreme Court of Thailand number 650/2532 (1989), Assistant Judges of the Supreme Court, 1st January 1990
- Decision of the Supreme Court of Thailand number 610/2539 (1996), Assistant Judges of the Supreme Court, 1st January 1997
- Decision of the Supreme Court of Thailand number 5161/2547 (2003), Assistant Judges of the Supreme Court, 1st January 1997
- Decision of the Supreme Court of Thailand number 4571/2556 (2013), Assistant Judges of the Supreme Court, 31 October 2014
- Decision of the Supreme Court of Thailand number 4893/2558 (2015), Assistant Judges of the Supreme Court, 21 October 2019
- Decision of the Supreme Court of Thailand number 12328/2558 (2015), Assistant Judges of the Supreme Court, 21 October 2019
- Decision of the Supreme Court of Thailand number 831/2559 (2016), Assistant Judges of the Supreme Court, 7 October 2016
- Decision of the Supreme Court of Thailand number 2600/2563 (2020), Assistant Judges of the Supreme Court, 1st January 2021
- Decision of the Supreme Court of Thailand number 3473/2563 (2020), Assistant Judges of the Supreme Court, 1st January 2021
- Decision of the Supreme Court of Thailand number 4189/2563 (2020), Assistant Judges of the Supreme Court, 1st January 2021
- Decision of the Supreme Court of Thailand number 79/2564 (2021), Assistant Judges of the Supreme Court, 1st January 2022
- Decision of the Supreme Court of Thailand number 4480/2564 (2021), Assistant Judges of the Supreme Court, 1st January 2022

International Case:

Smith and Others v Talktalk Telecom Group Ltd [2022] 1 WLR 5213

LIST OF STATUTES

Thailand

Constitutional Law 2017

Criminal Code (Penal Code) 2022

Civil and Commercial Code 2024

Civil Procedure Code 2017

Criminal Procedure Code 2019

Computer Crimes Act 2017

Cybersecurity Act 2019

Personal Data Protection Act 2019

Information Technology Act 1997

Electronic Transaction Act 2019

Consumer Protection Act 2019

The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society (Last updated March 2024)

Act for the Establishment of and Procedure for Intellectual Property and International Trade Court 2015

Act on establishment of Administrative Court and Administrative Court Procedure 1999

European Union

European General Data Protection Regulation 2016

Kingdom Saudi Arabia

Kingdom Saudi Arabia Anti-Cybercrime Law 2007

Kingdom Saudi Arabia Personal Data Protection Law 2021

LIST OF ABBREVIATIONS

AI	: Artificial Intelligence
ASEAN	: The Association of Southeast Asia Nations
AIS	: Advance Info Service
CCA	: Computer Crimes Act
CCC	: Civil and Commercial Code
CCIB	: Cyber Crime Investigation Bureau
CIA	: Confidentiality, Integrity, Accountability principles
CII	: Critical Infrastructure
CPC	: Civil Procedure Code
CSA	: Cybersecurity Act
CRPC	: Criminal Procedure Code
DDOS	: Distributed Denial of Service
DTRA	: Defence Threat Reduction Agency
DPIA	: Data Privacy Impact Assessment
DPO	: Data Protection Officer
EDPS	: European Data Protection Supervisor
EUGDPR	: European Union General Data Protection Regulation
ICL	: Islamic Criminal Law
ICT	: Information Communication and Technology
ID CARD	: Identification card
IOT	: Internet of Things
IT	: Information and Technology
LLM	: Large Language Model
MDES	: Ministry of Digital and Economy and Society
ML	: Machine Learning
NCSA	: National Cybersecurity Agency
NCSC	: National Cybersecurity Committee
NCRC	: National Cybersecurity Regulation Committee
NASA	: Nation Aeronautics and Space Administration
OTP	: One-Time Password
OCPB	: Office of the Consumer Protection Board
PDPA	: Personal Data Protection Act
PDPC	: Personal Data Protection Commission
TCAS	: Thai University Central Admission System
Thai CERT	: Thailand Computer Emergency Response Team
TNCA	: Thailand National Cyber Academy
WWW	: World Wide Web
UK	: United Kingdom

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The age of globalization has yielded significant growth with the advancement of technology, particularly in computers and internet connectivity. The internet and technologies, collectively are termed cyberspace,¹ are widely recognized and adopted by netizens worldwide. The paradigm shift in the transformation of transactions from offline to online platforms exaggerated the urgency to establish privacy rights prevalent to data subjects. Nevertheless, the bleak side of the internet is marked by illegal actions and unprecedented activities. For instance, the initial detrimental activities in the computer system include "Unauthorized accesses" or "Hacking,"² which damage the storage and interrupt or impair the functioning of the computer program system.³ Hitherto, technology progressed and evolved from local networks to worldwide connections through Online Networks.

This evolution influences how people as users engage with this online platform, whether for connecting or working, among other activities. Hence, the social network portal played an instrumental role in developing the concepts of personal data and personal data protection.⁴

¹ Jovan Kurbalija Eduardo Gelbstein, *Internet Governance Issues, Actors and Divides*, (Switzerland: DiploFoundation and Global Knowledge Partnership, 1st edn, 2015.), 5-21.

² Sawatree Suksri, *The Law and Regulations about Computer Crimes and Cybercrimes*, (Thailand: Faculty of Law Thammasart University, 2nd edn., 2020.), 61-70.

³ Sharon D. Nelson and John W. Simek, "The Anatomy of Data Breach", *Law Practice*, (2019), 38–41. Lawpractice, via Law practice, www.lawpractice.org.

⁴ Sneha Chawla, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments", (Unpublished Master's Independent Study Dissertation, Thammasart University, 2019), 74-77.

Processing personal data is crucial in achieving cyberspace activities, including but not limited to evaluating medical treatments through programming assessments. The significance of data storage can be gauged through the vulnerability of harm, through which sensitive information is exposed through data storage. Unauthorized Access⁵ refers to hacking or gaining unpermitted entry into a third party's system. This concept is directly proportional to the idea of a personal data breach, as statistical data analysed between 2015 and 2018 alludes to international collaboration enforced and initiated the implementation of the personal data protection agenda, as this activity expressly incorporated steps to counteract and prevent cybercrime.⁶ The Personal Data Protection statute emphasizes fundamental principles under the regulations for protecting personal data, which is the European Union General Data Protection Regulation (EUGDPR).⁷ This legislation significantly impacts the expansive, albeit extensive regional and global cooperation known as ASEAN. Thailand, as a member country of ASEAN, assimilated the concepts and principles since 2018. Thailand has recently implemented The Personal Data Protection Act (2019)⁸ to adopt EUGDPR's principles and the standard regarding data processing in cyberspace. The Thailand PDPA is a carbon copy of the legal adaptation of the EUGDPR.⁹

⁵ Sarawut Pitiyasak, *The Description of Thailand's Computer Crimes Act First and the Second Edition* (2007 and 2017), (Thailand: Nitithamlawbooks, 3rd edn., 2021), 56-60.

⁶ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136 Chapter 69 Gor). According to Remarks, legislators emphasize that it is necessary to declare PDPA as a personal data protection regulation to encounter personal data violations through data subjects in cyberspace.

⁷ 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) [. \(https://gdpr-info.eu/\)](https://gdpr-info.eu/)

⁸ Kanathip Thongveerawong, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, (Thailand: Nitithamlawbooks, 3rd edn., 2022),39-41.

⁹ Narong Jaiharin, et al., *General Data Protection Regulation (Thailand's description version)*, (Thailand: T.press Ltd., 4th ed.,2022), 1.

Nevertheless, the occurrence and escalation of personal data breaches pose a significant threat and risk to society globally. Personal data breaches significantly impacted Thailand. Subsequently, many industries, including but not limited to the corporate and the public sector, experience breaches and are exposed to valuable data breaches from their data storage portals.¹⁰ Ultimately, the culprit acquires access to sensitive data and exposed this confidential information to data harm through restricted platforms on the dark web for lucrative sales and trade.¹¹ Thus, in this illegal act, the perpetrators regarded this personal data as valuable for connecting to other cybercrimes, specifically identity theft, and ransomware, resulting in significant and severe consequences for the populace in Thailand.¹² Such circumstances inevitably lead to these inquiries and investigations.

1.1.1 Thailand's Personal Data Breach Situation

The Kingdom of Thailand's response to the issue of online defamation led to the revision and modernization of the Computer Crimes Act in 2017¹³ in anticipation of the

¹⁰ Personal Data Protection Act Thailand, "Summarizing: Thailand's Personal Data Breach Event 2018-2023", <<https://www.facebook.com/photo/?fbid=649740717170892&set=a.642220761256221>> (accessed 10 July 2024).

¹¹ Sharon D. Nelson, *The Anatomy of Data Breach*, 38.

¹² Bureau of Technology and Cybercrime, "The Research on the Effectiveness of Law Enforcement on Computer Crimes in the ASEAN Economic Community: A Case Study of Malaysia, the Republic of Singapore and the Republic of the Philippines". Department of Special Investigation Website, (Unpublished), 2021). 8-11. <https://www.dsi.go.th/th/Detail/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A8%E0%B8%B6%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%A7%E0%B8%B4%E0%B8%88%E0%B8%B1%E0%B8%A2%E0%B9%80%E0%B8%9E%E0%B8%B4%E0%B9%88%E0%B8%A1%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%AA%E0%B8%B4%E0%B8%97%E0%B8%98%E0%B8%B4%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9A%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%B1%E0%B8%9A%E0%B9%83%E0%B8%8A%E0%B9%89%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B9%80%E0%B8%81%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%A7%E0%B8%81%E0%B8%B1%E0%B8%9A%E0%B8%AD%E0%B8%B2%E0%B8%8A%E0%B8%8D%E0%B8%B2%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%84%E0%B8%AD%E0%B8%A1%E0%B8%9E%E0%B8%B4%E0%B8%A7%E0%B9%80%E0%B8%95%E0%B8%AD%E0%B8%A3%E0%B9%8C> . (Accessed 10 March 2024)

¹³ Sarawut, *The Description of Thailand's Computer Crimes Act First and the Second Edition* (2007 and 2017).

forthcoming Royal Decree Cybersecurity Act 2019¹⁴ and the Personal Data Protection Act 2019.¹⁵ Moreover, the proliferation and complexity of criminal activities, such as genuine fraud and defamation, have extended to the online platform. Furthermore, Thailand, alongside the rest of the world experienced the COVID-19 pandemic from 2020 to 2022, resulting in significant repercussions across all sectors of the economy. Thailand experienced notable personal data breaches in 2018, resulting in subsequent criminal activities.¹⁶ The following volume scales were implicated in the large-scale cybercrime incident involving the breach of personal data:

1. Crisis of personal data breach at Advance Info Service (AIS): In May 2020, the COVID-19 pandemic significantly worsened. A hacker infiltrated a sophisticated information service company specializing in high-quality telecommunications and premium telephone services. It was reported that 8.3 million internet records and papers from AIS's database were stolen.¹⁷ AIS boasts a prominent level of confidentiality and reliability, possessing Thailand's largest mobile number customers market share from 2015 to 2020. An effective coordination through internal cybersecurity effectively acquired and preserved the personal data of AIS on 22nd May 2020. Furthermore, as a consequence of this attack, AIS is apprehensive about the security of the internal system and aims to rectify both the cybersecurity of a domestic company system and the prevention measures for mobile use by implementing "double authentication" and "one-time password (OTP)" systems in financial transactions, as opposed to the previous

¹⁴ Government Gazette, Thailand Cybersecurity Act 2019, (2019). (Volume.136) (Chapter 69 Gor)

¹⁵ Government Gazette, Thailand Personal Data Protection Act 2019. (Volume.136) (Chapter 69 Gor)

¹⁶ The Bureau, "The Research on the Effectiveness of Law Enforcement on Computer Crimes..." .8-11.

¹⁷ *Bangkokpost*, "3-Week Lapse for AIS Data Breach", 2020, May 26., *Bangkokpost*, <https://www.bangkokpost.com/business/1924112/3-week-lapse-for-ais-data-breach>. (Accessed 15 April 2024).

design.¹⁸ However, it is undeniable that the AIS data leak led to the emergence of a sponsored criminal activity in Thailand called the "Call-Centre gang," which is accused of involvement in telephone fraud and has developed the reputation of profile scammers. Hitherto, this illegal activity has persisted through the Covid-19 pandemic until now.¹⁹ However, the AIS data breach attempt occurred during the PDPA and CSA frameworks already enforced. This incident should be investigated through this legislation, but the Act is still not fully enforced. Finally, AIS decided to provide tentative compensation to the clients who were violated according to the recorded report regarding the internal regulation under which AIS could treat the clients.²⁰ In conclusion, this crisis demonstrates that the major loophole in Thailand's legal system, through the gap between the theory and practice of the PDPA and CSA, is still not entirely effective.

2. The Data Breach catastrophe impacted ultra-sensitive corporations and the public sector. The Thai University Central Admission System (TCAS) was established in February 2022 under the auspices of the Council of the University President of Thailand, which operates under the authority of the Ministry of Education. The personal information of around 23,000 Thai students was leaked to the dark web (an underground marketplace where hackers illicitly sell personal data to other unauthorized individuals). Thai students' educational records and sensitive information on their identity cards (ID cards) were compromised and breached. The objective of this cybercrime is believed to

¹⁸ *National News Bureau of Thailand*, "AIS to Implement Additional Security Measures After Cyber Attack," 2022, *National News Bureau of Thailand*, February 22., <https://thainews.prd.go.th/en/news/detail/TCATG220222153051899>. (Accessed 15 April 2024).

¹⁹ The Bureau, "The Research on the Effectiveness of Law Enforcement on Computer Crimes...", 107-108.

²⁰ Udomtipok Praikaset Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya," Bangkok, (11 May 2024). Dr. Udomtipok provided information on the AIS crisis after the news report and silently discussed the situation. He addressed internal information and tentative compensation to AIS's clients, but any legal action against AIS has not been taken until now.

be the targeting of teenagers who are often not targeted and compromised to acquire personal information.²¹ Additionally, teenagers' consumption and use of technology can be examined. Consequently, it may motivate criminals to perpetrate this data breach at this incident.

The extensive personal data breach incident in Thailand, affecting private and public sectors, highlights such unlawful operations' far-reaching, detrimental, and grave implications. Furthermore, these incidents occurred prior to the declaration of the PDPA in Thailand in June 2022.²² Additionally, without specific regulations such as the PDPA, Thailand's Tort law principle treats injured persons inadequately. Moreover, it is undeniable that the negative aspect of technological advancement has a role in cybercrime, specifically in the form of personal data breaches.²³ This criminal action contributes to several other cybercrimes, such as online fraud, romance scams, ransomware, and similar offences.²⁴ Consequently, Thai legal frameworks should be concerned and vigilant about these cyber threats since they add intricacy to the process and persistently harm the community. This situation led to the initiation of this research to consolidate Thailand's legal provisions for addressing and safeguarding against criminal activities involving personal data breaches.

1.1.2 Brief Thailand's History of Legal Framework development in Personal Data Breach Crime

Thailand initiated the development of an information technology project campaign, which resulted in the enactment of the Information Technology Act (ITA

²¹ *Thairath Online*, "Another Day, Another Data Breach: Thai Students' Data Hacked, Sold on Dark Web", 2022, *Thairath Online*, February 4., <https://www.thairath.co.th/news/society/2305233>, (Accessed 15 April 2024).

²² Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 35-36.

²³ Xichen Zhang, et al., "Data Breach: Analysis, Countermeasures and Challenges", *Int. J. Information and Computer Security*, vol. 19 (2022): 402–442. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/365721658_Data_breach_analysis_countermeasures_and_challenges.

²⁴ Sawatree, *The Law and Regulations about Computer Crimes and Cybercrimes*, 99.

1997). In addition, the National Information Technology Committee was established on December 28, 2001, to supervise privacy issues. During the period between 2005 to 2013, Thailand's political climate allowed for the implementation of rules and regulations regarding private rights, as the ITA 1997. Before the pivotal coup d'etat in 2014, the National Legislative Assembly oversaw legislative discourse. As between 2014 and 2018, there was significant global advancement in incorporating the concept of privacy into the personal data protection perspective framework.²⁵ The passing of the European Union General Data Protection Regulation (EUGDPR), approved in 2016 and fully enforced in 2018, has significantly influenced cyberlaw causes worldwide. The implementation of the EUGDPR²⁶ has significant implications for various regions, including Thailand. There was an ongoing process (2017-2018) to develop and evaluate the adaptation of the EUGDPR into Thailand's legislation. Thailand announced the implementation of the Personal Data Protection Act (PDPA) 2019²⁷, through Article 32 of Thailand's Constitution of 2017²⁸, and the International Personal Data Transfer principles of the EUGDPR. This Act came into effect on June 1, 2022.²⁹

Despite the attempt to produce a personal data protection law, Thailand's legal framework for addressing personal data breaches between 2017 and 2021 relies on the Computer Crimes Act 2007³⁰ and the Penal Code³¹, which cover criminal offences, as well as the civil and commercial laws, encompassing elements of the General Tort Law.

²⁵ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 39-41.

²⁶ Narong, *General Data Protection Regulation (Thailand's description version)*, 99-102.

²⁷ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*.

²⁸ Thailand's Constitutional, (2017). (Volume 134) (Chapter 40 Gor)

²⁹ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, The attached appendix documents.

³⁰ Government Gazette, Thailand Computer Crime Act 2nd revision, (2017). (Volume 124) (Chapter 27 Gor) (Revised 2017).

³¹ Government Gazette, Thailand Penal Code. (Volume 139) (Chapter 28 Gor) (Revised 2022).

In 2010³², Thailand enacted a significant Royal Decree known as the Computer Crimes Act 2007 (CCA). The primary objective of this act is to elucidate specific criminal charges outlined in the Computer Crimes Act, specifically Unauthorised Access, which has been distinctively classified apart from Thailand's Penal Code in the realm of general criminal offences.³³ Given the prevailing conditions in Thailand, the cybercrime saga has been suppressed in a timely manner since 2015. Subsequently, this illegal activity mostly impacts offences such as online defamation, fraud, scams, and identity theft.³⁴ In addition, Thailand's CCA 2007 and Thailand's Penal Code are present to govern the prosecution and understanding of defamation offences committed on online platforms. In 2017, Thailand's legislature voted to revise and release the second edition of Thailand's Computer Crimes Act.³⁵ Furthermore, Thailand's significant legislative body has also approved the issuance of two Royal Decrees in 2019. The first one is for the Cybersecurity Act³⁶, and the Personal Data Protection Act³⁷.

The Personal Data Protection Perspective and the concept of data subject rights were discussed in 2019. The Cybersecurity Act³⁸ and the Personal Data Protection Act³⁹ were released to address shortcomings in data subject rights.⁴⁰ In addition, the PDPA enforces a wide range of legal measures, including three types of penalties: civil

³² Theerachit Jitkarunawong, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act And EU's General Data Protection Regulation (EUGDPR)", (Unpublished Master's. Independent Study Dissertation, Thammasart University, 2019).39.

³³ Suneti Kongthep, *Demonstrations of Thailand's Computer Crimes Act 2007*, (Thailand: Krungsiam Publishing), 2015.

³⁴ The Bureau, "The Research on the Effectiveness of Law Enforcement on Computer Crimes...".

³⁵ Government Gazette, Thailand Computer Crime Act 2nd revision. (Volume 124) (Chapter 27 Gor) (Revised 2017).

³⁶ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor).

³⁷ Government Gazette, Thailand Personal Data Protection Act 2019 (Volume.136) (Chapter 69 Gor).

³⁸ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor)

³⁹ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136 Chapter 69 Gor).

⁴⁰ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024 PDPA practitioners highlighted the main ineffectiveness of law practice: Thailand's population still lacks significant understanding in data subject rights exercises.

remedies, criminal charges, and administrative fines for non-compliance.⁴¹ Despite the complete implementation of the PDPA, the legal challenges surrounding personal data protection are still in their nascent phase. The legal system has been quantum-leaped in terms of readiness, responsiveness⁴², and organization in dealing with personal data breaches compared to 2017 and 2020.

The legislation in 2017, without the PDPA and CSA, acknowledges the injured individual as an injured person and ensures that the cybercrime perpetrator is prosecuted under the law. It can be demonstrated that numerous affected individuals experienced these illegal activities before the legislature and legal professionals became involved and enacted the necessary legislation, considering the prevalence of data breaches and the development of a legal framework. In addition, legal frameworks and processes conform to the fundamental primary laws specified in the general code Civil and Commercial Code⁴³ and Penal Code. Nevertheless, the Computer Crimes Act has been implemented and is undergoing amendments. In the penal code, the complexity and inconsistency between a particular offence and a general crime nevertheless overlapped and impacted criminal processes more efficiently than usual.⁴⁴ The anticipated enforcement of the Personal Data Protection Act, established by the Ministry of Digital and Economy, is expected to address legal concerns, enhance preventive measures against data breach crimes, and minimize the impact on affected individuals.

⁴¹ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 39-50.

⁴² Sawatree, *The Law and Regulations about Computer Crimes and Cybercrimes*, 112-115.

⁴³ Government Gazette, Thailand Civil and Commercial Code.(Volume 141) (Chapter 58 Gor) (Revised 2024).

⁴⁴ Worapit Meemak and Prapee Apichatsakol, "The Analysis of the Implementation of the Computer-Related Crime Act B.E. 2550", *Rajapark Journal* Vol.14 No.32 January-February 2020, vol. 14 (2020): 84–95. ThaiJo, via ThaiJo, <http://www.thaijo.org>.

1.2 PROBLEM STATEMENT

- (a) Thailand's personal data breach scenarios have consistently increased cybercrime frequency, as the entire data protection scenario.⁴⁵ As a counterfoil personal data violation, Thailand's private and public sectors were frequently harmed, and many people were affected by these invasions due to loss of privacy, financial interests, and illegal personal data disclosure. Furthermore, personal data breaches have reached an epitome as early as 2010 and continue to this day.⁴⁶ The background study demonstrates that even flagship organizations with high-level security were invaded and caused the explicit causation crime of identity theft. Therefore, this complicated cybercrime is considered a personal data violation activity, leading to this study.
- (b) Thailand's authority was overlooking personal data breach incidents arrangements. According to the background study, it could be determined that the peak level of personal data breach incidents was highlighted during Thailand's attempt to enact PDPA 2019, which is still in draft. Identity theft and online fraud are widespread as the consequences of personal data breach incidents during the COVID-19 pandemic.⁴⁷ Afterwards, Thailand's authorities operated an intense suppression scheme to halt identity theft and call centre *gangs*, which explicitly caused harm to Thailand's society. This strategy affected personal data breaches and seems to be overlooked by legal

⁴⁵ Personal Data Protection Act Thailand, Summarizing: Thailand's Personal Data Breach Event 2018-2023.<https://www.facebook.com/photo/?fbid=649740717170892&set=a.642220761256221>> (accessed 7 September 2024)

⁴⁶ Xichen Zhang, et al., Data Breach: Analysis, Countermeasures and Challenges: 402–442.

⁴⁷ The Bureau, "The Research on the Effectiveness of Law Enforcement on Computer Crimes ...". According to this study, the highlighted cybercrime is identity theft, and the study includes legal measures with other countries. However, personal data breaches are rarely mentioned.

practitioners. It is considered a typical hack, and the damages from this incident seem unimportant.⁴⁸ Moreover, the intense identity theft suppression scheme illustrates that Thailand's legal practitioners are oblivious to the new specific measures under the PDPA and the CSA, such as the notification principles and the subject of the amendment who complies with the latest legislation as the Data Controller.⁴⁹ Instead, the legal practitioners selected the complete legislation into practice, which are fundamental criminal offences in the Penal Code, CCA, and the general tort law principles in CCC, then selected the legal measures in PDPA and CSA. CCA does not explicitly criminalize personal data breaches, but it covers one of this cybercrime's components i.e. unauthorized access.⁵⁰ Thus, suppressing personal data breaches in Thailand seems non-imperative for two reasons: 1. The inaccurate suppression of Online Fraud but not emphasised personal data breaches and 2. Legal practitioners selected the fundamental legislation for the application rather than the specific Act, especially PDPA 2019 and CSA 2019, in the personal data breach incidents.

- (c) Thailand's data protection principles and personal data breaches are not widely known. The background study reveals that despite the legislators' efforts to implement the Personal Data Protection Act (PDPA) in 2019, several legal measures are in place to address the PDPA, including the

⁴⁸ Kiatchaloem Rakngam, "Legal Problem of the Determination of Offences Concerning Computer Access according to Computer Crimes Act", *Journal of MCU Nakhondhat*, vol. 7, no. 9 (2020): 193–204.ThaiJo, via ThaiJo, <http://www.thaijo.org> ., The author's problem statements. It emphasised that Thailand's Legal practitioners stick to implementing the law based on the Penal Code to suppress online fraud more than suppress unauthorised access related to personal data breaches in the duration before PDPA 2019.

⁴⁹ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*.,106.

⁵⁰ Kiatchaloem, "Legal Problem of the Determination of Offenses Concerning Computer Access According to Computer Crimes Act.",195-198.

Cybersecurity Act 2019 (CSA). These amendments necessitate the involvement of specialized units, experts, and specific legal measures, such as the notifications law and procedures for examining data controllers. Thus, in 2022,⁵¹ the PDPA's initial statement alluded to a restricted scope of personal data protection and personal data breaches, which was only comprehensible to experienced professionals. Therefore, the authorities have highlighted that the focus on dismantling *the call center gang* overlooked the significance of personal data breaches. Despite the full enforcement of PDPA in 2022, handling personal data breach situations under PDPA and CSA remains implicit. Moreover, in the event of a breach, the affected individual, as a data subject, may be uncertain and misguided while taking legal action. There is a lack of comprehension regarding the operational aspects of the PDPA and the CSA regarding personal data breaches, including exercising their rights in such cases.⁵² Hitherto, it is essential to comprehensively understand the legal paradigm of personal data breach incidents in the Kingdom of Thailand, including, but not limited to, legal professionals and the Thai population.

1.3 RESEARCH OBJECTIVE

- (a) To examine the characteristics and factors leading to personal data breaches in Thailand.

⁵¹ Thailand's PDPA Pro, " Thailand's Legislature Decided to Postpone Thailand's Personal Data Protection Act 2019 to 2022 due to reforming the private sector systems ", <<https://pdpa.pro/blogs/postpone-of-pdpa-and-guidelines>> (accessed 10 January, 2024).

⁵² The Office of the Personal Data Protection Committee (PDPC), Annual Report 2023 by Thailand Personal Data Protection Committee (PDPC), (The official office of the Personal Data Protection Committee (PDPC) website: 2024). <https://www.pdpc.or.th/pdpc-book/annual-report-2566/>. (accessed 15 April 2024)

- (b) To examine and analyze the existing laws in Thailand for reporting, preventing, and addressing personal data breaches.
- (c) To assess the effectiveness of preventive and responsive legal strategies in handling personal data breach offences in Thailand through a benchmark study between Thailand's PDPA 2019 and the EUGDPR 2016 framework.
- (d) To propose recommendations and suggestions to enhance the effectiveness of the legal measures for personal data breaches in Thai law.

1.4 RESEARCH QUESTIONS

- (a) What is the characteristic of a personal data breach according to the general and Thailand's perspective legal framework?
- (b) What are the current legal provisions in Thailand's legal framework related to personal data breaches?
- (c) What are the current strengths and weaknesses of Thailand's legal framework regarding personal data breach?
- (d) How does the availability and effectiveness of legal measures in the Thai legal framework compare to those in the European Union legal framework, as reflected in the EUGDPR?
- (e) Which aspect should be emphasized to enhance the efficacy of enforcing Thailand's PDPA and other significant measures related to personal data breach offences?

1.5 LITERATURE REVIEW

A relatively large number of sources have been examined to understand, clarify, and introduce the concepts, issues, problems, and solutions considered in this research. These sources, or rather their essence, which have massively supplemented the

researcher's knowledge and understanding of the issue, are reviewed here. The sources relevant to the topic of research relate to principles of Islamic law on data protection and its redress, international law, and sources on data protection and its redress in Thailand.

1.5.1 Nature and scope of personal data breach

This literature review will discuss and analyze the unique characteristics of personal data breaches, building upon earlier works such as documents, theses, independent studies, and journal articles. The aim is to present a comprehensive examination of this topic within the context of the dissertation. Firstly, this research aims to identify and elucidate the fundamental attributes of personal data breaches as described in several pieces of literature. Zahra Hassanzadeh and co-authors conducted experiments with the participants to analyze and obtain the fundamental perceptions of this cybercrime. This article provides a comprehensive summary of the unique characteristics and advancements of intentional personal data breaches, which are separate from the more usual hacking of computer systems. Moreover, this paper emphasized how to prevent and protect against unauthorized experimentation and cyber threats through collaborations. Therefore, this material will be further examined in the context of Thailand's specific circumstances and legal systems.⁵³

Historical examples and sample applications within the judicial process supported the actual experiments of personal data breaches. Michael Hopkins's article also comprehensively analyses the development of personal data breaches throughout history. Furthermore, the author critically analyses the repercussions of personal data

⁵³ Zahra Hassanzadeh, Robert Biddle, and Sky Marsen, "User Perception of Data Breaches", *IEEE Transactions on Professional Communication*, vol. 64, no. 4 (2021): 374–389. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/356685705_User_Perception_of_Data_Breaches.

breaches and concludes that personal data breach this crime is a precursor to identity theft and malware. The author suggests that addressing and combating this cybercrime is essential, as it operates as a chain and cycle originating from acquiring collected personal information, which is then used for other illegal purposes such as identity theft or online fraud. This article's narration was related to the personal data breach and will be examined in this study to provide a clear explanation from the perspective of Thailand.⁵⁴

In 2022, Xichen Zhang and co-authors discovered and released intriguing research that comprehensively summarises the uniqueness of personal data accessibility. The modern text provides a comprehensive overview of contemporary cybercrime, examines and describes the strategies and difficulties associated with combating this illicit activity. The authors comprehensively analyze this cybercrime, covering its upstream aspects (the parts of the data breach) and its downstream elements (the effects, responses, and difficulties posed by technological advancements in the future). This article aims to analyze Thailand's conditions, legal interpretation, and implementations, from the current substantive laws to the critique analysis of the conclusion.⁵⁵ Additionally, the theory has been widely circulated across the globe, as it correlated data breach with a netizen heritage. Nonetheless, the viewpoint is albeit a half-hearted theory regarding Thailand, as to call the culture an imperialistic one will be adding salt to injury for the many lies which already engulf Thailand.

Personal data breaches are recognized and addressed under the purview of general computer crimes, cybercrimes, personal data protection, and the Islamic

⁵⁴ Michael Hopkins, "Your Personal Information Was Stolen? That's an Injury: Article III Standing in the Context of Data Breaches", *The University of the Pacific Law Review*, vol. 50, no. 3 (2019): 427–452. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/340860788_Stand_in_the_Place_Where_Data_Live_Data_Breaches_as_Article_III_Injuries.

⁵⁵ Xichen Zhang, et al., Data Breach: Analysis, Countermeasures and Challenges. 402–442.

perspective. The Quran and Sunnah, the two sacred texts of Islam, specifically describe the substantive content related to this issue. The Department of Computer Science at the University of Bahrain conducted a study that examined the relationship between computer crime and the Islamic perspective based on the sources of Islam as the Holy Book Quran and Sunnah. This article explains personal data breaches in the current period, focusing on how they relate to Thai society, where most of the population follows Buddhism.⁵⁶

Personal Data Breaches originated from hacking and unauthorized access before the global recognition and enforcement of Personal Data Protection measures in 2014 to 2016. In his paper, Abdurrahman Bello Onifade and co-authors from the International Islamic University Malaysia (IIUM) elucidated the concept of computer crime and ethics from an Islamic standpoint, particularly emphasizing “hacking” discussed in the article. This elucidating analysis may be relevant to this study, incorporating insights from computer science and Islamic viewpoints. The overarching perspectives of both general and Thailand-specific contexts align with the perpetration of hacking and cybercrime involving personal data breaches.⁵⁷

Since 2015, the prevalence of cybercrime in Thailand has significantly escalated, resulting in substantial societal repercussions. The consequences of these actions have adversely affected the government and corporate sectors. The Bureau of Technology and Cyber Crime within the Department of Special Investigation conducted the report. In 2021, it showed a comprehensive analysis and examination of the legal

⁵⁶ Farvin, Shafinah, et al. Computer Crime from Islamic Perspective and the Role of Secure Software Practice to Mitigate Them,” in *International Conference on Social Sciences and Humanities | PASAK 2016*, organised by International Islamic University College Selangor, (Selangor: April 2016.), 412-425. <https://www.researchgate.net/publication/303551027>. (Accessed 15 April 2024).

⁵⁷ Abdurrahman Bello Onifade, et al, "Information Ethics: Islamic Perspectives on Privacy and Hacking", *Journal of Knowledge & Communication Management*, vol. 9, no. 1 (2019): 29–44. ResearchGate, via ResearchGate, <https://www.researchgate.net/publication/333510486>.

measures implemented in the ASEAN region. This paper comprehensively analyses the Computer Crimes Act, the operational procedures followed by Thailand's Special Division of Cybercrime Unit, and the cooperative efforts among ASEAN countries, including Malaysia and the Philippines. Nevertheless, the primary focus of this research centres around Identity Theft and Scammers, which refers to the interconnected cybercrime involving the unauthorized access and misuse of personal information. This report was released within Thailand's ongoing implementation of the Personal Data Breach Regulations, which still need to be fully implemented as of 2022. However, this article will analyse the Computer Crimes Act and examine the perspective of Personal Data Protection within Thailand's legal framework.⁵⁸

The Personal Data Protection Act (PDPA) is the sole legal Act that refers to a "Personal data breach." To gain a more accurate understanding of this cybercrime trait, it is imperative to apply the value of Personal Data Protection and Privacy to this study from the article. Sonny Zulhuda provides a detailed analysis of privacy and personal data from a legal standpoint. Furthermore, his work examines the Islamic perspective.⁵⁹ This demonstration aims to elucidate the personal data breach, which threatens societal privacy and may persist under Thailand's legal framework and measures, as discussed in this dissertation.

The phenomenon of Thailand's Personal Data Protection Act (PDPA) has been under discussion since 2015. The early enforcement of Thailand's PDPA has attracted the interest of an independent study conducted by Thammasat University. The study by Sneha Chawla focuses on transitioning from a privacy perspective to a personal data

⁵⁸ The Bureau, "The Research on the Effectiveness of Law Enforcement on Computer Crimes...".

⁵⁹ Sonny Zulhuda and Sidi Mohamed, *The Shari'ah Approach to Criminalise Identity Theft*, (Pertanika *Journal of Social Science and Humanities*: Universiti Putra Malaysia Press, Article in *Pertanika Journal of Social Science and Humanities*, 2015),169-181.ResearchGate, via ResearchGate, <https://www.researchgate.net/publication/316524215>.

protection perspective under Thailand's PDPA. This research examines the topic from both European and Buddhist viewpoints. This independent study focuses on the application of the Personal Data Protection Act, which is the primary legislation that directly addresses personal data breaches. Additionally, this study will compare the Buddhist religious perspective with the Islamic Perspective.⁶⁰

The “Cyber Law in Malaysia” book by Sonny Zulhuda and Ridoan Karim has many comprehensive descriptions, including the Cybercrime explanations, Personal Data Protection Principles elaboration, Cybersecurity narration, and the critical part of the future direction of the upcoming technology since 2020. Moreover, the book compares Malaysia's legal framework to Thailand’s PDPA 2019. Therefore, this updated publication in early 2024 and the inclusive description regarding the cyber law topic shall be fruitful and beneficial to this research. Also, some recommendations and suggestions from this book are highly likely to confront the development of Thailand’s legal framework.⁶¹

1.5.2 Legal Measures on Personal Data Breach in Thailand

Theerachit Jitkarunawong's examines a specific aspect of civil liability within Thailand's legal framework⁶², specifically the Personal Data Protection Act. The study also compares this Act with the European Union Association's EUGDPR. This research is highly advantageous for analyzing the specificities of civil liability within Thailand's comprehensive legal system. The focus of Thailand's Personal Data Protection Act (PDPA) is thoroughly examined in this article, providing a detailed analysis of civil

⁶⁰ Sneha, “The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments”.

⁶¹ Sonny Zulhuda and Ridoan Karim, *Cyber Law in Malaysia: Principal and Practices*, (Malaysia: Sweet and Maxwell, 2024).

⁶² Theerachit, “Civil Liability under Data Protection Law: A Comparative Study of Thailand’s Personal Data Protection Act and EU’s General Data Protection Regulation (EUGDPR)”.

liability within Thailand's legal framework. Specifically, it explores the relationship between the general civil and commercial code and the unique substantive law, the Personal Data Protection Act. This research will provide valuable insights into Thailand's legal framework, specifically focusing on civil liability. It will continuously explore two other areas of interest: criminal sanctions for personal data breaches and administrative fines.

Thailand's Personal Data Protection Act (PDPA) was formulated and implemented in 2022, serving as an additional legislative measure already in effect. However, between 2011 and 2017, although these legal measures were available, their execution was not expected until personal data breaches were explicitly violated and online fraud exacerbated the spread in Thailand. Implementing the Computer Crimes Act has raised significant concerns. Furthermore, the inconsistencies between online distortions and illegal activities defined by Thailand's Computer Crime Act were resolved between 2014 and 2015. Thus, Thailand's second modification of the CCA was implemented in 2017. Nevertheless, the loophole in personal data breaches and this Act (unauthorized access) persists today. The situations and the development of this legislation and measures are explained in detail in the articles written by Thanonthat Suthariyanitipakdi⁶³ and Kiatchaloem Rakngam.⁶⁴ These documents will help analyse

⁶³ Worapit, "The Analysis of the Implementation of the Computer-Related Crime Act B.E. 2550", 84–95. The author addressed the problem statement as the legal practitioners selected the fundamental criminal offences in the penal code more than CCA. Moreover, from the study, the author highlighted the ineffective law implementation as the definition in penal and CCA that the data and personal data are not covered. Thus, the exercise of this legislation could not succeed in terms of a personal data breach.

⁶⁴ Kiatchaloem, "Legal Problem of the Determination of Offenses Concerning Computer Access According to Computer Crimes Act". In this study, the author addressed the contradiction between the definition in CCA and the penal code of data, which is directly affected in section 14(1) of CCA and the offences in the penal code that the fake data (involved in more than one offence). Moreover, the exercises in the penal code more than the CCA affected the effectiveness of law implementation. Also, PDPA and CSA overlook implementation through specific cases, especially personal data breaches.

Thailand's legal efforts on criminal sanctions in response to personal data breaches in this research and analyze them systemically with another legal measure.

It is essential to examine existing literature explaining the law's substance to gain knowledge about Thailand's legal system and the application of law in actual lawsuits. This will allow for a comprehensive analysis and conclusion of the research. Several books provide detailed explanations of substantive law and practical instances. Firstly, one such book was authored in 2020; Sawatree Suksri's book comprehensively depicted cybercrime.⁶⁵ In the author's book, the author discussed the prominent features of hacking, which include unauthorized access and personal data breaches. These aspects represent the progression of cybercrime from 1980 to 2019. In addition, the author conducted comparative research on Thailand's legislative framework, the German legal framework, and those of selected legislations to investigate and evaluate the existing legislative measures related to personal data breaches. This analysis of cybercrime from Thailand's standpoint will be further explored, examined, and compared to the other information and legal measures in this research.

Thailand's Computer Crimes Act, or CCA, is an essential legal measure that should be emphasized and enforced against individuals who have breached personal data. As Sarawut Pitiyasak described, this Act provides a comprehensive framework for addressing such offences. Sarawut Pitiyasak's book⁶⁶ focuses on the evolution of this act and examines the critical revisions made to this substantive law. It discusses the second revision in 2017 and explores the relationship between CCA and the Cybersecurity Act 2019. This cybersecurity legislation strengthens and upholds the "national cybersecurity perspective and policy," thereby improving the interpretation

⁶⁵ Sawatree, *The Law and Regulations about Computer Crimes and Cybercrimes*.

⁶⁶ Sarawut, *The Description of Thailand's Computer Crimes Act First and the Second Edition (2007 and 2017)*.

and implementation of the law. Moreover, this book compares the Cybercrime Convention of 2001, one of the legal statutes that impacted the CCA. This statute, in turn, influenced the first modification of CCA in 2007. The description of CCA can also be found in the works authored by Phaijit Sawadisarn⁶⁷ and Suneti Kongthep's books.⁶⁸ However, Sarawut's book provides more substance and explicitly explains the relationship with substantive law. These books exemplify one of Thailand's legal measures (CCA), which will be further demonstrated and analyzed with specific legislation such as PDPA and CSA in this investigation.

The "Personal Data Protection Act" enacted by Thailand in 2019 and wholly enforced in 2022 is another legal measure distinguishing between unauthorised access and personal data breach. This legislation ensures privacy and personal data protection by defining a personal data breach" as the unauthorized access and illegal acquisition of personal information. Kanathip Thongveerawong's book⁶⁹ provides an in-depth analysis of Thailand's legal framework, technology law, and perspective on personal data protection, including a comprehensive overview of PDPA 2019. The author's analysis of PDPA is thorough and precise. Furthermore, the book's author also provided explanations and comparisons with the EUGDPR legislation, comparing the legal framework to PDPA. However, most of the book's content centres around the rights and responsibilities of the data subject, data controller, and data processor in collecting and processing personal information under a legitimate purpose without explicitly emphasizing the concept of personal data breach. However, it is crucial to apply this

⁶⁷ Phaijit Sawadisarn, *Computer Usage in Legal Practice and Laws Related to Computer*, (Thailand: Chuanpim 50 ltd, 5th edn.), 2014.

⁶⁸ Suneti Kongthep, *Demonstrations of Thailand's Computer Crimes Act*, (Thailand: Krungsiam Publishing), 2015.

⁶⁹ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*.

legal remedy in the description of the research, along with other pertinent legal measures, to address this cybercrime.

Thailand's PDPA 2019 structure includes a specific legal provision for addressing personal data breaches. These measures were adopted from the EUGDPR and were also implemented in a law known as the "Data Breach Notification Law." It is worth noting that this law was initially enforced in the United States of America as it served as a model for other countries. The Notification law mandates that the "Data Controller" must inform the personal data owner when a breach occurs and also offer tentative compensation for the incident. This information not highlighted in Kanathip's PDPA book, authored by Chawin Aunpat, thoroughly depicts this action, highlighting that Thailand had not yet implemented the "Data Breach Notification Law"⁷⁰ then. Thus, this research aims to satisfy a significant additional legal measure requirement regarding personal data breaches and address the affected individual, as illustrated in this existing research.

The primary source for benchmarking study regarding legal measures to address and mitigate personal data breaches is the European General Data Protection Regulation (GDPR), enacted in 2016 and fully implemented in 2018. While many literature discusses this legislation concerning comparison and standards, it does not explicitly address the personal data breach issue. Previous studies have mainly focused on the Personal Data Protection Act. The author has narrated and translated the EUGDPR into Thai language. Narong Jaihar and his co-authors released the book before the PDPA was implemented in 2021. The book provides valuable insights and comparisons of the legal measures between Thailand's PDPA and EUGDPR. This study shall continue in

⁷⁰ Chawin Aunpat, "Data breach Notification Law", *Thammasart Law Journal (Anniversary 60th years of Assoc.Prof. Suda Wisarupich)*, (2015): 277–287. ThaiJo, via ThaiJo, <http://www.thaijo.org>.

the benchmark analysis and make further recommendations to develop Thailand's legal system.⁷¹

Lastly, Philip Treleaven and his co-author released research⁷² in 2023 that thoroughly explains the function of Artificial Intelligence (AI) and cybercrime. Their research also includes a pertinent analysis of personal data breaches. This article explores the inclusive content that examines the involvement of AI and cybercrime in personal data breaches and other criminal activities. AI can facilitate crimes such as identity theft by generating "Deepfake" or "Target" voices to impersonate individuals and manipulate victims into illegally acquiring assets. Similarly, Carla Lozonschi's article⁷³ gave a significant opinion that AI might act as a cybercriminal assistant through the advancement of this thing. This research will criticize personal data breaches and the high potential of these developments in the context of Thailand's society. Early research was implemented and predicted the future direction of cybercrime in Thailand, which faced the growth of cybercrime from general unauthorized access to personal data breaches and continued development from personal data breaches into AI-assisted criminals committing these illegal activities.

1.6 RESEARCH METHODOLOGY

The research conducted in the legal doctrinal study and employs library research. The methodology deals with the letter-of-the-law to legal issues, adducing to pure theory than practice. The main objective of this study is to investigate the characteristics of personal data breaches in Thailand. Moreover, this study comprehensively examines

⁷¹ Narong, *General Data Protection Regulation (Thailand's description version)*.

⁷² Philip Treleaven, et al, "The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami", *University College London*, (2023): 1–34. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/372399289_The_Future_of_Cybercrime_AI_and_Emerging_Technologies_Are_Creating_a_Cybercrime_Tsunami.

⁷³ Carla Lozonschi Irina Bakhaya, "Artificial Intelligence and its Impact on Cybercrime" in *The International Conference on Cybersecurity and Cybercrime 2023 organized by the Romanian Association for Information Security Assurance*, vol. 10 (Bucharest: Publisher, 2023), 120–126. .

the legislative provisions on personal data breaches inside Thailand's legal system. Additionally, it will conduct a benchmarking analysis of the legal frameworks of the European Union. The current legal framework in Thailand encompasses various legal measures to address the crime of personal data breaches. These measures contain criminal penalties, civil liability, and administrative non-compliance sanctions. It is important to note that Thailand is still in the initial phases of enforcing the Personal Data Protection Act and the relevant legislation enforced under personal data breach incidents in Thailand.

Additional issues discussed include the preconceived notions in the backdrop of such violations, including the emulated methods, and the unrealistic opposition to such initiatives by all stakeholders. Data collection for this study will be obtained from primary and secondary sources. To illustrate, the primary source focuses on domestic and international laws, official legal documents, and Thailand's official law reports. Simultaneously, supplementary information from books will be collected. Internet resources shall provide links to relevant journals, articles, papers, manuscripts, news, official academic seminars/webinars, and other written documents. Furthermore, the data was collected through interviews with Thailand's legal practitioners. This data collection collected in-depth information regarding 1. Thailand's personal data breach situations, 2. Thailand's legal framework analysis and opinions regarding implementation issues, and 3. Recommendations and Suggestions for improving Thailand's legal application comprehensively. Afterwards, these interview collection data will be summarised, translated into English, and demonstrated as a legal opinion report under the doctrine documents. These legal practitioners' opinion reports are attached to this research after the references.

Finally, the data analysis will utilize both resources to assess through legal analytical and critical approaches to understanding personal data breaches from a general to a detailed perspective. The objective of this study is to examine and apply legal provisions within the legal framework of Thailand. Legal measures employ established general to specific legal measures to comprehensively analyse and decipher various legal documents, ranging from overarching regulations like Constitutional law to specialized statutes such as the Personal Data Protection Act. Furthermore, Thailand's official law report shall demonstrate the directions of law interpretation and implementation, which is beneficial for analysis in the practice of the current amendments. The outcome is expected to be in terms of advantages and loopholes through the legal analysis to improve Thai law comprehensively. In addition, Secondary Resources will incorporate a critical analysis section that draws upon the literature study to evaluate the current legal measures for this specific cybercrime.

1.7 SCOPE AND LIMITATION OF STUDY

This legal doctrinal study will examine the distinctive characteristics of the offence of personal data breach are many circumstances and implications in Thailand and globally. One such limitation at this point may astound the reader: Data breach cannot be given to trouble-making scammer outfits to broadcast their nonsensical tirades. On the contrary, all matters should be regulated about what nonsense has been disseminated, and a counter-argument should be enforced against all malpractices.

The Personal Data Protection perspective examination will consistently broaden and consolidate the existing legal safeguards to prevent any violation of Personal Data in Thailand's legal framework. This research will expand the benchmarking analysis to

include the EUGDPR⁷⁴, which impacts Thailand's PDPA⁷⁵ Through several legal frameworks. This research aims to find legal strategies to address, anticipate, and combat the crime of personal data breaches. This research will analyse the legal measures within the specified framework, specifically concerning the familiar concept of personal data protection in legislation. Upon a personal data breach, it is anticipated that a comprehensive evaluation of legal measures and benchmarking analysis will be conducted, resulting in recommendations to improve the existing legislation.

However, this research limitation shall be considered the limited sources of references. Firstly, Thailand's legal system is in its nascent execution phase, especially PDPA 2019 and CSA 2019, which were just implemented in the first three years. Moreover, the official law report under Thailand's Personal Data Protection Act and Cybersecurity Act by Thailand's Supreme Courts is still in process for official publication⁷⁶. Thus, the official law report under Thailand's judiciary shall be demonstrated through the primary legislation, such as the Penal Code, CCC, and CCA, until 2021 (published in 2022).⁷⁷ Likewise, the PDPC's specific authority is to examine and determine the law under PDPA, so the official law report regarding PDPC is unavailable in this doctrinal study.⁷⁸ Secondly, the secondary reference source, especially the legal elaboration under the CSA 2019 amendment description book, is unavailable. Thus, Thailand's Cybersecurity Act 2019 will be described primarily based on the legislation. Also, the subordinate legislation under the Ministry of Digital

⁷⁴ 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)
<https://gdpr-info.eu/>

⁷⁵ Government Gazette, Thailand Personal Data Protection Act.(Volume.136 Chapter 69 Gor)

⁷⁶ Court of Justice of Thailand, Thailand's Official Law Reports in Data Breach Case (Non-translation).
<http://www.supremedekacourt.co.th> (Accessed 15 April 2024).

⁷⁷ Ibid.

⁷⁸ Annual Report 2023 by Thailand Personal Data Protection Committee (PDPC).

Economy and Societies (MDES) is still producing other secondary legal measures, which this study will refer to until March 2024.⁷⁹ Nevertheless, this research compiled all the data based on the Thailand legal practitioner's opinion in the Appendix. It is sufficient to analyse and provide recommendations and suggestions to achieve the research objectives.

1.8 CHAPTERISATION

The research is divided into five chapters. Chapter One commences with the research proposal, which encompasses the background of the study, problem statement, research questions and objectives, literature review, research methodology, and scope and limitations of the study.

Chapter Two explains the general characteristics of this specific cybercrime. Continuing with the elaboration from the perspective of Islamic criminal law, this section will emphasize the features of personal data breaches. Furthermore, the perspective on personal data protection further elucidates the significance of safeguarding the offender's personal data target. It also outlines the overarching objective of the general unique data protection viewpoint: to address and mitigate the societal impact caused by cybercrime effectively.

Chapter Three provides a summary of Thailand's legal system measures regarding personal data breach incidents. This study aims to provide a concise overview of the conditions, particulars, and ramifications of the unauthorized disclosure of personal data. This study focuses on constitutional law until specific legislation is created to protect personal data. Furthermore, this study analyses Thailand's legal

⁷⁹ Thailand's Ministry of Digital Economy and Society. (MDES) and Government Gazette, The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update March 2024, (2020). <<https://www.mdes.go.th/law>> (accessed 15 April 2024)

framework by examining its civil and commercial laws and Penal Code concerning personal data breaches. This analysis focuses on both tort law and criminal law. This research demonstrates the specific Acts that address personal data breaches: the Computer Crimes Act and the Personal Data Protection Act. This chapter will provide a concise overview of the comprehensive legislative mechanisms within Thailand's legal framework to address personal data breach incidents.

Chapter Four focuses on the specific legal measures emphasized in analysing the interpretation and implementation of personal data breach issues within Thailand's Legal Framework. This chapter's contents refer to what has been stated in this dissertation. Moreover, this chapter examines the strengths and shortcomings of Thailand's current legislative measures. The purpose is to illustrate and explain the functions of these legal measures, both in terms of legislation and practical application, in the event of this specific cybercrime. Moreover, this chapter analyses and compares Thailand's legal provisions with those of the European Union General Data Protection Regulation (EUGDPR). The benchmarking study is expected to demonstrate parallels and differences and provide interesting recommendations for interpreting and implementing legislative measures to address personal data breach offences. Furthermore, considering forthcoming legislation and the evolving landscape of global technology, this chapter examines the role of Artificial Intelligence (AI) and crimes related to the breach of personal data.

Chapter Five provides a conclusion by discussing the characteristics of personal data breaches. This chapter contains concise conclusions, and this section should encompass an analysis of the legal context. This conclusion section includes the benchmark analysis result and the critique component of the research on the growth of legal measures. This chapter provides recommendations and suggestions for both the

research findings and Thailand's legal practitioners' opinions to enhance the effectiveness of implementing a legal framework inclusively regarding personal data breach incidents.

1.9 SIGNIFICANCE OF THE STUDY

This study is believed to serve as the initial step in analysing, examining, and modifying Thailand's legal framework on the crime of Personal Data Breach. This study concept could be assimilated, executed, and adapted to Thailand's legal framework for application in actual legal proceedings and litigation. In addition, the study of Thailand's Personal Data Protection Act primarily emphasizes civil actions outlined in Section 4 of the PDPA, and the liability for data breach offences is still restricted. Consequently, this approach could address a deficiency in the field of cyberlaw research. In addition, cyberlaw in Thailand is relatively new and has excellent growth potential thanks to the early and comprehensive adoption of research in this area. This can significantly contribute to the development of cyberlaw as an academic discipline at Thailand law school. Eventually, this study collected interest metrics that still need to be employed inside Thailand's legal framework and system. These recommendations, which are part of benchmarking research, aim to advance Thailand's laws in the field of cyberlaw by amending and refining the existing legal statutes. Lastly, this legal doctrinal study can improve Thailand's global competitiveness and enhance public trust towards the global economies.

CHAPTER TWO

PERSONAL DATA BREACH: NATURE, DEVELOPMENT, AND THE LEGAL ISSUES IN ISLAMIC CRIMINAL LAW PERSPECTIVE

2.1 INTRODUCTION

Chapter Two explains the characteristic features of the personal data breach from a standard point of view, accompanied by an intricate study of the nature of this phenomenon from an Islamic perspective. The central theme of chapter two is spirited around the idea of outlining the well-versed norms, including but not limited to the salient features of a personal data breach, prior to examining the core operator status based on the teachings of Islam. In the past decade, the Kingdom of Thailand has experienced significant harm on a widespread scale due to cybercrime, particularly during the hiatus between 2018 and 2020.¹ Furthermore, the impact of cybercrimes persists, and the individuals responsible for these illegal acts have made notable advancements in technology and the intricate process of carrying out this breach.

Post Advance Info Service and TCAS incidents during 2019-2021 could be assessed; the scope of certain variable issues was to be determined amid the hindsight of these incidents in the pre-PDPA and CSA enforcement. From the highlighted incidents effectively to the social intensely, the absence of a genuine regulation means the Kingdom of Thailand's population lacks trust in the cybersecurity system to maintain security and safety.² Such circumstances allude to a massive responsibility to

¹ Statista Research Department, "Number of Breached Online Accounts in Thailand From 1st Quarter 2020 to 2nd Quarter 2023", <<https://www.statista.com/statistics/1404553/thailand-number-of-account-breaches-exposed/>> (accessed 2 August 2024). According to the records, the highest breach of data in Thailand was in 2020, with more than 4000 data illicitly disclosed on illegal platforms.

² Personal Data Protection Act Thailand, "Summarizing: Thailand's Personal Data Breach Event 2018-2023", <<https://www.facebook.com/photo/?fbid=649740717170892&set=a.642220761256221>>

undertake knowledge of these incidents inclusively, whether suppression of cybercrime, settlement of personal data protection personnel and the standard of the settlement of cybersecurity system adequately, as observed in the restructuring in the internal system through the provisions of the tentative payment in AIS incident as elaborated in Chapter One. However, after Thailand's PDPA and CSA promulgation as the milestone, a personal data breach incident occurred in 2023.

2.1.1 Recent Case of Personal Data Breach in Thailand

The 9 Near Crisis occurred between mid-March and April 2023. A hacker whose alias was 9 Near claimed to have obtained data on behalf of Thailand's population, a total of 55 million people, and threatened to reveal it. The proclamation led to widespread chaos, causing acute alarm across the Kingdom. This threat was substantial, enabling personal data loss to be a more vulnerable element than the AIS problem of 2020.³ The Ministers of the Ministry of Digital Economy and Society (MDES) assisted during these circumstances. Furthermore, this investigative operation was supported by a well-structured special police unit, the Cyber Crime Investigation Bureau (CCIB), established between 2020 and 2022 in conjunction with another unit prior to the enforcement of the PDPA, which came to the rescue of the masses. The preliminary inquiry unravelled the identity of 9-Near. To the earnest shock of the nation, the person turned out to be military personnel who possessed and acquired tech-savvy computer and technology skills. The investigation revealed that 9 Near's girlfriend happened to

(accessed 10 July 2024). AIS is the flagship telecom service provider company that had data breached in 2020. Afterwards, the online fraud spread after 6 months from this incident. This incident was believed to be the primary breach of connectivity that cybercrime spread in Thailand. Meanwhile, the TCAS incident is an early example of the government sector that was invaded by data disclosure of students' data. (TCAS is the university examination unit under the Ministry of Education)

³ *Amarin TV*, "'9 Near' เป็นใคร? ทำไมยังจับไม่ได้? จำสิบโท ดกข้อมูลคนไทย 55 ล้าน" (Who is 9-Near? Why could the authorities not arrest him? Sergeant Major Second Class stole Thailand's population 55 million.), *Amarin TV*, 2023, April 8. <https://www.amarintv.com/spotlight/economy/detail/44003> (Accessed 15 April 2024)

be a nurse knowledgeable of the internal access gateway to the hospital's database system.

Recently, 9 Near publicly disclosed that he possesses personal data, alluding to sensitive data, including but not limited to addresses and mobile phone numbers.⁴ His claims ranged from collection of data truly breaching the government code locks of data protection excessing public sector data, potentially furthering cybercrimes, including but not limited to ransomware, malware and data breach to profit financially, surpassing the threat posed by 9 Near. According to the report, 9 Near Operation fiasco commenced in mid-March 2023 and concluded in early April 2023.

The Cybersecurity committee officer received a message from 9 Near, leading a joint investigation to collaboration between the ministry, CCIB, and the Cybersecurity committee. The base domain of 9near.org in Thailand was tracked, and the website was shut down, exposing the cyber-criminal's location. Despite the cyber-criminal's desperate attempt to appear as launching the cyber-attack from overseas. Furthermore, it was suggested by 9 Near's girlfriend, who worked to be a nurse and supported the medical officer's official Facebook fan page, that 9 Near may have accessed the original database from the previous government application called "Mor Phrom" (Doctor is Ready). This application operated during the COVID era (2019-2022).⁵ A comparison between 9 Near's announcement and the data from the Mor Phrom application revealed that Thailand's data, holding an aggregate of around 54.1 million people, was used to manage second vaccine doses and monitor public movement during the continuing COVID-19 lockdown.

⁴ Ibid.

⁵ Ibid.

The Mor Phrom application is no longer available as the system has been deactivated. The government officer's combination operation was successful within two weeks of recognizing the 9 near domains. On 9 April 2023, 9 Near decided to surrender himself, and his girlfriend followed suit on 12 April 2023.⁶ This case is prosecuted under a specific military court based on 9 Near status. Moreover, the Data controller (hospital) might also be subjectives under the PDPA and CSA provisions. Nevertheless, the Minister publicly announced that 9 Near is liable under Thailand's CCA and PDPA (primarily for the first time post-PDPA enactment).⁷

Thailand's awareness of the impending cyber-attack depicted the lack of surveillance and due diligence during the severe cybercrime crisis in 2023. Prior to the enforcement of PDPA and amid an epitome of personal data breaches, Thailand's Legal Framework encountered challenges related to Personal Data and ensuring proper cybersecurity compliance, which prompted the problem statement of the dissertation. The study demonstrates the salient features of the PDPA, examining characteristic patterns with the actual circumstances through the application of PDPA articles when applying the characteristics in the mentioned content, including but not limited to the combination of cybercrime, unauthorized access, and Personal Data Breach. Additionally, an initial investigation revealed that 9 Near was a highly skilled campaigner in computer technology and ranks Sergeant Major Second Class in the Thai army. His accomplice holds the position of an internal officer in the organization. Thus,

⁶ *Thaipbs world*, "มอบตัวแล้ว “จ่าสิบโท” แฮกเกอร์ “9Near” 9-Near already surrender himself to the authority", *Thaipbs world*, 2023, April 12. <https://www.thaipbs.or.th/news/content/326573>. (accessed 15 May 2024).

⁷ *BBC Thai*, "9near : จับกุม จ่าสิบโท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว" 9-Near surrender himself the hacker who claimed that earned 55 million record of Thailand's population data", *BBC Thai*, 2023, March 31. <https://www.bbc.com/thai/articles/cq5z3w5lwdx0>. (accessed 15 May 2024). According to the minister's statement, he emphasized that 9 Near shall be liable for unauthorized access offenses with the increasing punishment of 9 Near invading the Critical Infrastructure facility (medical services). Also, PDPA criminal liability sanctions should be addressed in the case. However, recently, 9 Near has been under military court proceedings.

based on the individual's professional status, it may be concluded that prior to initiating the invasion operation, the cyber-criminal cautiously studied the system and carefully planned the strategy for several weeks.⁸

According to the analysis from the Ministry of DES and CCIB division, 9 Near may have had a strong interest in becoming a political activist after surrendering. CCIB and DE intend to emphasize the initiation on an operation that will be launched to illegally purchase personal data. This aim addresses the past general characteristics and the ongoing condition of the Call-Centre Gang, which had been operating constantly since the peak of the personal data breach. The central analysis of this crisis focus on Thailand, as the country experienced personal data breaches in both technical and non-technical forms. This included crimes such as theft of personal information, unauthorized access to personal data, and the illegal sale of personal data by former officials. If 9 Near had already exposed data from two-thirds of the people on the Dark Web, the potential damages could have risen to hundreds of million Baht.⁹ This case is anticipated to serve as an imperative example for future studies on personal data breaches and cybercrimes at Thailand's law schools, following the “official legislation report”.

In short, Thailand's personal data breach scenario can be categorized into two phases: 1. pre-PDPA enforcement, and 2. Post PDPA enforcement (since June 2022). Furthermore, comparing the overall characteristics and the current personal data breach scenario in the preceding chapter reveals striking similarities. However, the distinction

⁸ *Amarin TV*, "'9 Near' เป็นใคร? ทำไมยังจับไม่ได้? จำลึบโท จกข้อมูลคนไทย 55 ล้าน" (Who is 9-Near? Why could the authorities not arrest him? Sergeant Major Second Class stole Thailand's population 55 million.), *Amarin TV*, 2023, April 8., 2023, April 8. <https://www.amarintv.com/spotlight/economy/detail/44003>. (accessed 15 May 2024).

⁹ *BBC Thai*, "9near : จับกุม จำลึบโท แสกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว" (9-Near the criminal claimed that hold Thailand's population data for 55 millions records got caught already.), *BBC Thai*, 2023, March 31. <https://www.bbc.com/thai/articles/cq5z3w5lwdxo>. (accessed 15 May 2024).

lies in Thailand's non-technical personal data breach or internal unauthorized access, a data leak.¹⁰ Moreover, incidents can be divided into two categories based on the operations:

1. External threats, as demonstrated in AIS and 9 Near incidents, as the perpetrator accessed personal data without the prior consent of the data subject and through obtained personal data and

2. Internal Threats committed by the perpetrators, who are the internal personnel in the victim's organisation.¹¹ The operation uses non-technical tactics, not relying on computers and technology. Several hackers are internal organisations that obtained personal data illegally, sold it on illegal platforms for perks, and leaked highly sensitive personal data to third-party operatives. The accused were prosecuted through court proceedings.

Data breach is the pinnacle of imperative loopholes due to the technological quantum leap of post-modern times. Any compromised set of data plays a critical role for the enormous populace. Social media platforms, including but not limited to Facebook, Instagram, X (formerly Twitter), Snapchat, and chatbots like Chat GPT are comprehensively utilized for sharing snaps, building online friendships, dating, identifying lost old friends, and releasing updates. As well as social platforms have the capability to influence people's lives, including exposing the privacy of others without their consent; they have grave consequences for society.¹² Data breachers create

¹⁰ Sawatree Suksri, *The Law and Regulations about Computer Crimes and Cybercrimes*, (Thailand: Faculty of Law Thammasart University, 2nd edn., 2020.),100-123.

¹¹ Personal Data Protection Committee Thailand, "ขายผล ทลชเครือข่ายซื้อขายข้อมูลส่วนบุคคล ใน PDPA OPERATION EP.7" (PDPA operation Ep.7: Thailand's authorities expanding the operation to suppress the illegal purchasing of personal data.), <<https://www.pdpc.or.th/4174/>>. (accessed 15 May 2024).

¹² A. V. Rajan, R. Ravikumar and M. A. Shaer, "UAE Cybercrime Law and Cybercrimes — An Analysis" (paper presentation), *International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*, London, UK, 2017), 1-6,<https://doi.org/10.1109/cybersecpods.2017.80748>.

nuisances as they use confidential data for their own ulterior motives tantamount to privacy breach through the processing of sensitive data through harm, distortion, public disclosure, and abuses. This activity is considered as one of the crimes that take economic, social, and legal issues into consideration. Firstly, in economics, it is predictable that post an incident occurs, personal data misuse always follows, which in Thailand could explain why Call-Centre Gang operated this invasion prior to committing Online Fraud, which affects the loss of hundreds of millions of baths from the victims of the cyber-criminal. Moreover, Thailand's continuous suppression of Call Centre Gangs since 2021 and root cause could be determined, and the root cause of personal data gained came from AIS incidents.¹³

Secondly, from a social perspective, personal data breaches directly affect the reputation and trustworthiness of private and government organizations. Specifically, since the TCAS incident, many government organizations have faced the side effects of continuous cyber attacks, unauthorized access, and distributed denial of service (DDOS); these have disrupted the system and destroyed the availability of government services operations. Additionally, these unlawful activities have caused the decreasing trustworthiness among Thailand's population to the government sectors and authorities in terms of inclusive operation to detect and suppress these illegal activities. Specifically, in personal data breach incidents during 2020-2022, there are no intense legal actions to these circumstances. Thus, Thailand's population as the Data Subject under PDPA fell unsecured and requires the appropriate safeguard and reliable measures in both prevention and suppression from the continuous cyber attack.¹⁴

¹³ Patipon Wongsrikul, "อาชญากรรมทางไซเบอร์ในประเทศไทย (Summarize Thailand's Cybercrimes Situations)", *INTERRISK ASIA (THAILAND) CO., LTD.*, 2022, June 6. <https://www.interriskthai.co.th/th/cybercrime-in-thailand/> (accessed 1 August 2024)

¹⁴ Ibid.

Finally, legal issues in Thailand are primarily concerned with pre-PDPA enforcement incidents, such as specific measures namely the Notifications Law; the responsibility for remedying the incident post the incident occurs is unavailable. Nevertheless, as the Post-PDPA and CSA enforcement incident, Thailand has successfully handled and not only caught 9 Near (offender) but the PDPA and CSA also approached these circumstances by the responsible organization inspecting the compliance duty by the authorities. Based on Thailand's milestone, the personal data breach incident, the discussion shall continue highlighting the characteristics of personal data breach elaborations.¹⁵

2.2 THE NATURE OF PERSONAL DATA BREACH: FACTORS AND MANNERS

In general, a personal data breach is considered as an Information Theft. However, the scope and definition of personal data breach shall be narrower than information theft by the category of personal data, which shall be specific information that could be defined as people or humans. Meanwhile, information, by its nature, could be interpreted in terms of product, Intellectual Property, blueprint, and any information that does not involve personal data.¹⁶

Such incidents could demonstrate that several personal data breaches are committed by hackers involving cybercrime and computer misuse. Including the operation of obtaining illegal access to personal data in the storage into usage for malicious purposes, which occurred in internal organisations, as exclaimed in terms of

¹⁵ Worapit Meemak and Prapee Apichatsakol, "The Analysis of the Implementation of the Computer-Related Crime Act B.E. 2550", *Rajapark Journal* Vol.14 No.32 January-February 2020, vol. 14 (2020): 84–95. ThaiJo, via ThaiJo, <http://www.thaijo.org>.

¹⁶ Sonny Zuhuda, "Information Security in Malaysia: A Legal Framework for the Protection of Information Assets," (Unpublished Ph.D. thesis, International Islamic University Malaysia, 2010)., 217-245. This thesis was written when Malaysia's PDPA enforced this threat, which was recognized as the term information theft.

“Insider Threats.” Moreover, personal data breaches generally cover unforeseen incidents that do not involve cyber-criminals but could be determined from human errors and the system (Technical).¹⁷ Tentatively, the nature of a personal data breach can be divided into three main segments: external operations, internal operations, and accidental circumstances.

2.2.1 External Operation

Firstly, the perpetrators severally committed personal data breaches through Unauthorized Access, which operated as a multi-layered cybercrime due to illegal access requiring multiple instances of malicious computer misuse.¹⁸ The operation primarily involves imposing malicious software, such as viruses, trojans, etc. This cybercrime is thought to evolve alongside technological advancements. The criminal primary action stated will impact the outcomes of assaulting, compromising, and sabotaging the security system. To demonstrate, the cybercriminal deploying Malware to turn off the firewall or antivirus of a target system temporarily, exploiting vulnerabilities to allow criminals to breach the database quickly or execute cybercrimes such as ransomware to encrypt and seize data as leverage, breaching the security system to perpetrate personal information stolen.¹⁹ Cybersecurity is the primary function of preventing fraudsters from obtaining personal data through unauthorized access and breaches.

¹⁷ Kanathip Thongveerawong, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, (Thailand: Nitithamlawbooks, 3rd edn., 2022), 375-380.

¹⁸ Zahra Hassanzadeh, Robert Biddle, and Sky Marsen, "User Perception of Data Breaches", *IEEE Transactions on Professional Communication*, vol. 64, no. 4 (2021): 374–389. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/356685705_User_Perception_of_Data_Breaches.

¹⁹ Ibid. “The data presented in this article are derived from 35 one-on-one, in-person sessions with participants about their mental models of internet data breaches. Each session lasted 40 to 90 minutes. Participants were compensated with a small monetary payment. This study was reviewed and cleared by a university Research Ethics Board.” The authors presented semi-practical experiments to determine the user's tentative understanding of when the cybercrime happened.

The pathway to committing a personal data breach is determined by the categories of personal data breach by technical, explicitly referring to the vulnerability of the cybersecurity system. Cybercriminals shall struggle to use malicious software to examine and identify vulnerabilities in the target system.²⁰ The analysis identifies the primary security vulnerabilities as administrator access, user access, and backdoor access.²¹ Intensely breach the system by compromising the complete antivirus and firewall system, going beyond a broad breach. Thus, the key activities involved in cybercrime to access this gateway are phishing, identity theft, and spam, which often serve as the principal support for this operation. Criminals sometimes pose as administrators to covertly infiltrate databases, as any cybersecurity alerts would shorten the window for leaking personal data.

The data-trace should be easily traceable. The significant realm for cybercriminals to focus on is backdoor access, which may be identified by the presence of malware and collaboration with cybercriminals after the system is compromised, leading to a prolonged recovery process.²² Therefore, the preparedness and accessibility of the security system are crucial in many personal data breach scenarios, especially when the victim's system is obsolete or not up to date, according to both the victim's and the cyber-criminal's perspectives. The problem of identity theft alludes has far-reaching effects and implications that may occur chronologically illustrated in the following ways:

- Unauthorized acquisition, control, or possession of personal information through various ways such as stolen computers, lost identification cards,

²⁰ Sharon D. Nelson and John W. Simek, "The Anatomy of Data Breach", *Law Practice*, (2019), 38–41. Lawpractice, via Lawpractice, www.lawpractice.org.

²¹ Hassanzadeh, "User Perception of Data Breaches", 374-389.

²² Ibid., 385-389.

hacking or unauthorized access of computer system, ATM scanning, data leak or phishing.

- The fabrication of fake accounts and documents based on personal information so wrongfully acquired. The design includes acquiring counterfeit credit cards, ATM cards, e-mail accounts, social networking accounts, loan applications, banking transactions, etc.
- Converting the above document or transactions into a certain gain, both monetary and non-monetary. This occurs when the data thief manages to obtain bank loans, withdraw money from the ATM or online banking, surfs and opens and shops using counterfeit credit cards, con others to execute certain payments, or even to execute a property transfer to a third party.
- Alternatively, counterfeit documents or accounts may be used to launch some other forms of crimes such as money laundering, extortion, cyber-bullying, defamation, computer sabotage or spamming.

2.2.2 Internal Operation (Insider Threat)

The preceding passages reveal to us how different incidents with multiple wrongdoings can lead to identity theft. It has many faces or elements of different crimes. Hitherto, it is a fraudulent act, alternatively categorized under stealing or instead a trespass or a misuse of personal documents. Data acquired from an alien electronic system, involves unauthorized access and when the data is in the non-computerized document it is simply a theft or misappropriation of property. Identity theft is therefore commonly characterized by the resulting event, and not through its origin. Identity theft is therefore

unlawful collection, use or processing of personal information for the purpose of obtaining certain gains from the perpetrator or causing certain losses to others.²³

With this definition, identity theft is vulnerable to both criminal and civil liabilities. Laws of crime and torts may therefore come into play when they fit into the particular facts of each case. This is why the word “theft” had been replaced in some literature by word “fraud” or merely “abuse” in order not to constrain it under the domain of criminal laws.²⁴

Personal data breaches can also occur in non-technical ways, like physically destroying hardware systems and databases, as the outcome of spreading personal data on illegal and public platforms without protection and consent. These breaches can happen in non-technical environments due to technological loopholes such as bug vulnerabilities in the system, power outages, and security system failures. The Non-Technical individual should focus on the evidence indicating that Public Services in Thailand acted in bad faith by leaking data to a Call Centre gang for financial gain.²⁵ This analysis suggests that this criminal activity stems from the original crimes perpetrated by individuals with malicious intent to disrupt peace and order within society. This sample could fall under the "Officer wrongfully exercises his function" crime in Thailand's Penal Code²⁶ and related violations. Personal data breaches

²³ Gottschalk, Petter. “Categories of Financial Crime.” *Journal of Financial Crime* 17, no. 4 (October 12, 2010): 441–58. Emerald Insight, via Emerald Insight, <https://doi.org/10.1108/13590791011082797>.

²⁴ Francis Fukuyama, *The Great Disruption: Human Nature and the Reconstitution of Social Order*, (United States of America: Free Press; First Edition, 2000).

²⁵ *Thaipbs world*, "Hai Officials Arrested for Selling Personal Information of Over 1,000 People to Call Centre Gang", *Thaipbs world*, 2022, October 29, <https://www.thaipbsworld.com/3-thai-officials-arrested-for-selling-personal-information-of-over-1000-people-to-call-centre-gang/>. (accessed 15 May 2024).

²⁶ Government Gazette, Thailand Penal Code.(Volume 139) (Chapter 28 Gor) (Revised 2022).

Section 157 From this event, it could be expected that the offender will be subjected to another offence, such as Thailand's Computer Crimes Act. The combination of criminal offences in the Penal Code is also the internal measure for the administrative law sanction as the offender is the government officer. Moreover, it is believed that this case is under procedure processing, which could be expected to be the official law report in the future.

typically involve technical means, such as a computer, to commit cybercrimes. This often occurs through unauthorized access to personal data stored in online cloud storage, reflecting the advancements in Internet technology and cyberspace. Several cases of personal data breaches are related to technical means.²⁷

As mentioned above, this category was conducted based on the breach of secrecy in both physical and technical activities. Insider threats committed by several hackers have already gained access due to the cybercriminals initially can be internal organization personnel. After gaining access to the storage a disclose personal data illegally sold to other cybercriminals or spread to third parties without the organization or client's permission.²⁸ It is considered that this category requires comprehensive legal measures, which Thailand conducted on the original criminal offences rather than implementing PDPA and CSA, which were enacted in terms of cyberspace. Nevertheless, if the cyber-criminal uses a computer to commit a personal data breach. Then, this issue will be dealt with under PDPA and CSA, and the organisation where management of the personal data is also subject to legal compliance issues.

2.2.3 The Threat of Personal Data Security and Non-Malicious Incidents

The personal data breach and unauthorized disclosure have gained popularity and created massive public concerns among consumers in these following years. Personal data breaches are not a new case as in early 2012, telecommunication companies were reported to leak millions of their customers' personal data to third parties. As economic globalization and trade liberalization developed and engineered by the massive and rapid development and innovations of technologies and Internet, data breaches continuously create main users' public concerns all over the world including Thailand.

²⁷ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 375-380.

²⁸ Patipon Wongsrikul, อาชญากรรมทางไซเบอร์ในประเทศไทย (Summarize Thailand's Cybercrimes situations).

Media also played their role in reporting more and more cases for unauthorized data leakage and data breaches occurred on a surprisingly massive scale. Considering Internet development and big data collection, dire needs for personal data protection are now a main concern of Internet users and customers of business industries. Subsequently, the issue addressed that a commission was established to monitor its compliance; the occurrence of many personal data breaches on a massive scale created doubt on the effectiveness of the commissioners' enforcement to prevent noncompliance under the legislation. Hence, it is a need to review the enforcement mechanism. Subsequently, to prevent undesired cases of data breaches and ensure full compliance of business and industries players.²⁹

The characteristics of personal data breaches could be directly implemented with a personal data protection perspective, clearly mentioning that this incident involved cybercrime through the malicious use of computers, presenting a threat to system security. This phenomenon pertains to the primary risk of breaching confidentiality (secrecy). The risk of Integrity (accuracy) amid the detrimental impact of personal data availability (readiness) relates to the personal data security principle of the CIA.³⁰ The CIA framework, which stands for Confidentiality, Integrity, and Availability, emphasizes the mandatory compliance required by the data controller and data processor in protecting personal data. It involves implementing essential security measures, notifying individuals during a security breach, and offering potential compensation to affected data subjects.³¹ It explains the extensive damage caused through breach of confidentiality, compromising data integrity, and making personal data unavailable, leading to potential financial, safety, and mental losses due to

²⁹ Ibid.

³⁰ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 381-385.

³¹ Ibid.

cybercriminal activities. Including, The losses of the organization's reputation and untrustworthiness from the consumers and users through losses vide the security system breaching.³²

Continuously, personal data breaches could illustrate the factors and threats that launched the operations; due to the high value of personal data in cyberspace, cybercriminals likely have malicious intentions to commit cybercrimes. The intention of these cybercriminals is as follows:

1. Financial profit derived from the correlation between data breaches and identity theft. This unlawful action caused the misuse of personal data and provided continuous online fraud, which is less processed and earned financially swiftly. Moreover, identity theft and online fraud caused significant challenges regarding forensic identity challenge, which caused the victims to face difficulties in getting inclusive treatment.

2. Personal data breach is one of the categories of information theft, whether in conjunction with other criminality like malware or not.³³ This is reflected in the high reputation of the target and the price of personal data that the organization kept, especially sensitive and biometric data. Espionage is a primary incentive for hackers to access systems to obtain sensitive and highly classified information and establish a reputation for skill. It targets the top three organisations: healthcare facilities, financial

³² Xichen Zhang, et al., "Data breach: Analysis, Countermeasures and Challenges", *Int. J. Information and Computer Security*, vol. 19 (2022): 402–442. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/365721658_Data_breach_analysis_countermeasures_and_challenges. According to the summarisation report, it could be seen that the damage evaluations shall be in "overall" actual calculations such as the contamination in cybersecurity, the specifically identified losses of personal data, both the standard and biometric sensitive data and so on. For example 2019, the Facebook data breach cost around 5 billion US dollars. Capital One data breach could be predicted to be damages of approximately 300 million us dollars, and the Equifax data breach in 2017 caused total evaluation damages of around 1.4 billion us dollars compared with 147.9 million injured persons. [the information from the paper's summarization table pages 430-431]

³³ Sharon D. Nelson, "The Anatomy of Data Breach".38–41.

institutions, and critical information infrastructure (CII) units.³⁴ Moreover, the priceless value of personal and biometric data alluring cyber criminals operating in large-scale organizations determines the possibility of success and the quantity of personal data in storage. Thus, it is not a surprise that Advance Info Service, the leading telecom service provider as a CII unit, faced a significant data breach in Thailand in 2020.

However, when considered inclusively in terms of a personal data breach, even primarily caused by the hackers, it is undeniable that such an undesirable outcome could occur accidentally, which may not involve cybercrime or cybercriminals directly; hence, it is termed a non-malicious personal data breach incident. This phenomenon could happen due to uncontrollable due to the Force Majure³⁵, primarily when natural disasters, accidental processing, and human and data controller system errors occurs. For instance, the company enfaced a thunderstorm on that day, causing the internal system to function abnormally; then, with the dysfunction, the data processors transmitted the wrong set of clients' data inaccurately and disclosing in-depth personal client data on the company's website. This instance demonstrated that the mistake of revealing confidential personal data might have caused without invasion or intrusion from outside or internal personnel who possessed unauthorized access. This accidental breach shall be examined regarding proper security and the data controller's responsibility under EUGDPR principles.³⁶

In short, this part illustrates the inclusive personal data breach operation, prinarily committed by the person and accidental circumstances. Several incidents

³⁴ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor) Section 3

³⁵ Government Gazette, Thailand Civil and Commercial Code. (Volume 139)(Chapter 69 Gor)(Revision 2022) Section 8.

³⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Article 4 (12).

involve computer misuse, and cybercrime focuses on unauthorized access and continues with multiple operations. Thus, the CIA's principal application in PDPA and CSA become the specific amendments that emphasize compliance duties and the responsibility to uphold and arrange the security system to prevent and detect this threat³⁷, which the description shall be in the next chapter.

From the significant personal data breach circumstances to nature and the distinctive, the next part shall elaborate on one of the essential principles based on the Islamic perspective. To expand the area of this dissertation and examine the interpretation and implementation of personal data incidents in unique directions, the religious perspective of Islam is the focal pivot of this dissertation.

2.3 PERSONAL DATA BREACH UNDER THE ISLAMIC CRIMINAL LAW PERSPECTIVE

The Islamic faith has a distinct and unique character that guiding Muslims to follow the straight path through the primary guidelines of the way of life known as Shariah.³⁸ "The "Shariah" institute play a rudimentary role in regulating Islamic Law to govern and influence Muslim behaviour in both the present world “Dunya” and the afterlife “Aqirah”.³⁹ Islamic Law possess various categories, including Islamic administration and Governance and Islamic Law in Banking and Finance. The primary category associated with this infraction is Islamic Criminal Law (ICL).⁴⁰ Maqasid-Al-Shariah

³⁷ Thailand National Cyber Security Agency, Annual Report 2022 by Thailand National Cyber Academy (TNCA), (Thailand National Cyber Security Agency official website, 2023).https://ncsa.or.th/Ebook_%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A/files/basic-html/page1.html (Accessed 15 April 2024).

³⁸ Muhammad Akram Laldin, *Introduction To Shari'ah And Islamic Jurisprudence*, (Malaysia: Cert Publications, 2015).1-14.

³⁹ Ibid.

⁴⁰ Rudolph Peters, *Crime and Punishment in Islamic Law, Theory and Practice from the Sixteenth to the Twenty-first Century*, (United States of America by Cambridge University Press, New York: Cambridge University Press, 2005), 9-20.

is the central core rudimentary principle implemented prior to the enactment of a legal statute based upon five core elements.

1. Religion
 2. Life
 3. Dignity
 4. Intellect
 5. Property
- These five central cores shall conduct Muslim behaviours and uphold social harmony.⁴¹

These principles show that Islamic Law has a distinct and comprehensive system that governs both behaviour and spiritual guidance to help believers attain the ultimate goal of eternal paradise (Jannah). Furthermore, the thesis outlines the legal right to consent and privacy of netizens who might be oblivious to the respective guidelines for data protection and the research gap on damages through data breaches in actions resulting from social media. Theoretically, the background is based upon Islamic theory as an Islamic framework. Legal theory is a collective manifestation of the respective boundaries in the field of privacy, data breach, and acquired damages.⁴²

2.3.1 Information Security Perspective between Islam and Buddhist Faith

The “Shariah” enacting as the primary source of Islamic Law is based on the holy book Quran and the “Sunnah” of Prophet Muhammad SAW. Significantly, the Islamic Perspective elaborate on the teachings of “Privacy” and “Secrecy”, which are related to the CIA principle known as Information Security.⁴³ These are mentioned in both the

⁴¹ Muhammad Akram Laldin, *Introduction to Shari'ah and Islamic Jurisprudence*, 14-18.

⁴² Ibid.

⁴³ Sonny Zuhuda, "Information Security in the Islamic Perspective: The Principles and Practices", (paper presentation, Proceeding 3rd International Conference on International Conference on Information and Communication Technology for the Muslim World Jakarta, Indonesia (ICT4M 2010), organized by IEEE Indonesia Section, [et al.], (Jakarta, December 13-14, 2010): 33-39 . https://www.researchgate.net/publication/224251211_Information_security_in_the_Islamic_perspective_The_principles_and_practices. (Accessed 15 May 2024).

rudimentary principle and the Islamic punitive measures (Taziraat) in the Holy Book of the Quran as follows.

*“O, you who believe! Do not access houses other than your own until you have asked permission and saluted the dwellers therein; that is best for you, Allah admonishes you, so that you may heed.”*⁴⁴(Qur'an, 24:27-28)

*“Avoid suspicion, for airing suspicion, is the most lying form of speech.”*⁴⁵(Qur'an, 49:12 in part)

The enactment of PDPA is an action of government to show its seriousness in protecting the right to privacy as it is a fundamental right entrenched in many international human rights instruments. The right to privacy exist not just as a mere human right but in some scope, is also developing as a cause of action in the law of tort. The right of privacy has also been approved in Islam as contained in the primary source of Islamic law which is the Holy Quran.

As Allah the Almighty states in Surah al-Hujurat verse 12 , *"Oh you who believe! Avoid suspicion as much (as possible): for suspicion in some cases is a sin: And spy not on each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it... But fear Allah: For Allah is Oft Returning, Several Merciful."* (49:12)⁴⁶

The scope of the applicability of PDPA in Thailand is not absolute as the legislature provides few exceptions. For example, in Section 3 of the PDPA 2019. Since the Act itself did not clarify nor categorize of which person, institution, statutory body, agency, or any other persons may be regarded as part of government for the purpose of

⁴⁴ An-Nur: 27-28.

⁴⁵ Al-Hujurat: 12.

⁴⁶ Al-Hujurat: 12.

getting an exemption from the applicability of PDPA upon it, the assignment shall discuss about the kind of person(s) that may be claimed as part of the government.

Moreover, Prophet Muhammad SAW also emphasized the importance of privacy as a right that people should follow and respect, protecting the confidentiality, classification of information, and secrecy between parties and stakeholders. One of Hadith refers to the above issue is on follows;

*“Who came to know the secret of a person and conceals it is like who gives life to a buried girl.”*⁴⁷

Several verses of the Holy Quran could be demonstrated explicitly emphasizing the importance of secrecy, which is interpreted in conjunction with the term “confidentiality” and also includes the specific purpose of communication and transmission. The verse also highlighted maintaining the truth and avoiding “lying”. This principle could be interpreted as effective communication as developed into the Integrity or accurate principle regarding information security principles.

*“We (Muslims) are the last (to come) but (will be) the foremost (on the Day of Resurrection)...If someone is peeping (looking secretly) into your house without your permission, and you throw a stone at him and destroy his eyes, there will be no blame on you”*⁴⁸

These principles, rooted in the Islamic perspective, demonstrate that interpretation and execution are considered rudimentary aspects of privacy as a human right in the Universal Declaration of Human Rights (UDHR).⁴⁹ Furthermore, this

⁴⁷ Abu Dawud, *Sunan Abi Dawud*, Riyadh, Darussalam Publishers, 1st Edition, 2008, Hadith No. 4891, 307.

⁴⁸ Al-Bukhari, *Sahih al-Bukhari*, Riyadh, Darussalam Publishers, 1st Edition, 1997, Hadith No. 6887, 87.

⁴⁹ UN General Assembly, Resolution 217A (III), Universal Declaration of Human Rights, A/RES/217(III) (December 10, 1948). Article 12

principle was incorporated into the personal data protection standards of the CIA to ensure confidentiality, which aligns with Islamic principles which emphasis on safeguarding classified information.⁵⁰ The information and data must be readily available with accuracy and integrity for correct and precise utilization. The Islamic legal system contains comprehensive frameworks that cover the interpretation of rudimentary rights to address the crime of personal data breach.

The Islamic perspective emphasizes a comprehensive structure that provides guidelines for humanity, unlike the "Buddhist" perspective in Thailand, where several of the population follows Buddhist teachings. Buddhism emphasizes purifying the mind through meditation and the concept of Individualism, which involves isolating oneself to meditate and cleanse the mind of sinful thoughts and behaviors. *The Five Skandhas* in Buddhist teachings elucidate the origins of *Thkua* (Form, perception, violation, emotion, and consciousness or six senses⁵¹) to distinguish between body and mind. These principles reflected the "Right to be let alone" or the isolation from the publicity and disclosure of behaviors, information, or any activities necessary. Interpreting the significance of privacy rights via practicing and understanding Buddhist teachings is an indirect approach.

The Buddhist teachings emphasized individualism and focused on cultivating the soul and mentality to accomplish the ideal of true liberation of the soul, known as *Nirvana*.⁵² Moreover, Buddhist religious teachings were distinctly divided into

⁵⁰ Mohammad Hashim Kamali, *Right to Life, Security, Privacy and Ownership in Islam*, (United Kingdom: Islamic text society, 2008). Chapter 3,153-232.

⁵¹ Sneha Chawla, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments", (Unpublished Master's Independent Study Dissertation, Thammasart University, 2019), 48-52.

⁵² Ibid. ,48-55. The privacy right under the Buddhist religion mainly occurs in terms of training behaviors and spiritual minds through individual activity, especially meditation. All of this spiritual training to overcome all sinful thoughts and actions. Furthermore, the highest achievement of this training is "Nirvana."

instructions for the Monk and the Secular, with interpretation primarily geared toward the teachings of the Monk. When comparing the teachings of Buddhism related to religion, Buddhists will understand privacy through prayer and meditation, as well as the essential guidance provided by the five basic precepts for the secular aspect.⁵³ Islamic religious system is more direct and concise than that of Buddhism. The Islamic perspective established the essential structure as the systematic law, and the guideline is more precise based on the legal foundation.

The Western legal systems, especially Britain and France, has affected legal evolution in Thailand since King Rama V's reign (AD 1868-1910), when the Kingdom of Siam preserved sovereignty during the colonial phase by France and Great Britain. Thailand implemented the modern legal system and adopted the Civil Law system as its primary legal framework.⁵⁴ Since its inception, Thailand's legal system has affected Western legal concepts and systems. It has implemented them following the general theory of the privacy perspective, such as the Right to be let alone by Daniel Solove⁵⁵, and the value of privacy espoused by Ruth Gavison and Judith Jarvis Thomson.⁵⁶ Afterwards, physical privacy was developed through the "Legal transplantation" methodology, and it became the personal data protection principle Thailand adopted and enforced in PDPA.

⁵³ Ibid.

⁵⁴ Ibid.,11-15.

⁵⁵ Ibid. "1. The Right to Privacy 2. Personal Information Management 3. Personhood, 4. Intimacy, 5. Limited Access to the Self, 6. Secrecy. Stefano Scoglio also defines informal privacy as "Physical Privacy," connected to the concept of "a man's house is his castle." It pertains to the category of ownership of our bodies. Privacy is a distinct value safeguarded by a shield of property. 2. Decisional Privacy pertains to an individual's choices and decisions regarding their private conduct. Personality rights typically safeguard this domain. 3. Informational Privacy: This aspect of privacy pertains to information management. It pertains to the knowledge that others possess about an individual. Currently, privacy mostly pertains to informational privacy. Formational Privacy pertains to actions like advertising that infiltrate an individual's mind. Delving into someone's head is another way of invading their privacy". The description can be found on pages 11-12.

⁵⁶ Ibid.,11-13

In conclusion, Islam implements and interprets the rudimentary principles of privacy and information security explicitly and directly from the primary source of law. Meanwhile, Thailand's legal framework adheres to the interpretation and application of laws based on the general theory and the Western legal system.⁵⁷ The Islamic perspective adheres rigorously to its unique framework, resulting in a specific interpretation and implementation of regulations. This is evident in the display of the ICL perspective and the current condition of personal data breaches.

2.3.2 Current status of interpretation direction in ICL Perspective

According to Islamic Criminal Law, infractions might be classified into three main categories. The first category is *Hudud* or *Hadd* crime, which pertains to a distinct group of offences with predetermined punishments in Islamic law. *Hudud* offences are primarily interpreted and implemented from the primary source of law in Islam, such as the Quran and Sunnah, which involves retaliation, and the second category, *Tazir*, which includes other measures.⁵⁸ The *Hudud* criminal categories are specific infractions defined and punitive according to primary sources of law, such as the Quran and Sunnah (teachings and actions of Prophet Muhammad SAW). This category includes seven offences, which are related to and closely resembles the feature of a personal data breach. These criteria indicate the "Illegitimate obtaining of personal data" described by Sariqah.⁵⁹ Examining the discovery and comprehending the relationship between interpreting and implementing theft (Sariqah) and personal data breach components is essential. Sariqah, or the theft offence, is classified as a *Hudud* crime in Islamic penal law. Anwarullah (2008) and Paizah (1991) found that sariqah means possessing

⁵⁷ Sawaeng Boonchalermwipas and Atiruj Tunboonchareorn, *The Thai Legal History*, (Thailand: Winyuchon, 20th edn., 2022). ,49-55 and 227-236.

⁵⁸ Anwarullah, *The Criminal Law of Islam*, (Malaysia: A.S Noordeen, 5th edn., 1997).,174-180.

⁵⁹ Islamonline, Theft via the Internet and the Application of Hadd., <<https://fiqh.islamonline.net/en/theft-via-the-internet-and-the-application-of-hadd/>> (Accessed 11 March 2024)

someone else's property without permission.⁶⁰ The fundamental principle established in Surah Al-Mai'dah (5):38 of the Holy Quran states that.

*“As for the thief, male and female, cut off their hands. It is the reward of their deeds and exemplary punishment from Allah. Allah is Mighty wise.”*⁶¹

An action must meet the required elements to be considered a Hudud crime. The Sariqah has the essential requirements to deal with and enforce laws against cybercrime, such as personal data breaches.

1. The cyber-criminal responsible must have stolen the item covertly.
2. The thing stolen by the criminal must have value or be movable.
3. The perpetrator must unlawfully take possession of the owner's property, and the stipulated punishment in the Holy Quran, which includes severing the cyber-criminal's hand, may be enforced.⁶²

This offence procedure is based on Shubhah or "doubt" in determining guilt by presenting required evidence components. Hand amputation cannot be enforced as a penalty if the theft involves tampering with evidence or essential parts of the crime.⁶³ The Shubhah principle could be implemented so that if any doubts occur, even if the components of Sariqah are fulfilled, the offence of Sariqah could not be established. Instead, new criminal categories called Ta'zir could be established, which include penalties such as execution, imprisonment, and administrative fines. The Ta'zir categories intricately demonstrate government control at its discretion, such as the sanctions specified in the Anti-Cybercrime Law in Saudi Arabia (2007).⁶⁴

⁶⁰ Anwarullah, *The Criminal Law of Islam*, 174-180.

⁶¹ Al-Mai'dah: 38

⁶² Rudolph Peters, *Crime and Punishment in Islamic Law, Theory and Practice from the Sixteenth to the Twenty-first Century*, 53-56.

⁶³ Ibid.

⁶⁴ Kingdom of Saudi Arabia Anti-Cybercrime Law, (Act. No. A/90)(Reprint 2007) (2007). Article 3

Anwarullah (2008) and Paizah (1991) defined Sariqah in the context of *Hudud* criminal crime as the unauthorized act of surreptitiously taking someone else's property.⁶⁵ According to this definition, a personal data breach is when personal data is stolen. Cybercriminals usually sell stolen personal data on the dark or deep web for nefarious purposes following a data breach. Sariqah elements might be categorized as a Personal Data Breach depending on the nature of the conduct.⁶⁶ The cyber criminal's first aim is the "database system," a highly secure and complicated system protected by cybersecurity developers. Furthermore, individuals can only oversee extensive information and personal data in this highly secure storage system. This natural safeguard fulfills the Hirz obligation according to the legal perspectives of Imam Shafei and Ahmad, Abu Hanifah, and Imam Malik.⁶⁷

The unauthorized acquisition of personal data through a personal data breach meets the criteria of "property" concerning the information owned by the individual data owner or protected by the "data controller." This suggests that the property referred to, specifically the "personal information," must be recognized and satisfied. Furthermore, using the Qiyas or analogy method in understanding the law aids in linking Theft and Personal data were stolen.⁶⁸ This is especially imperative when considering cyber thieves' aim to acquire "financial gain" by stealing credit card information. Once the prerequisites of Sariqah are met, the robbery is considered complete, even if the stolen information is intended for further malevolent activities.⁶⁹ The evidentiary criterion for addressing a personal data breach can be satisfied using a

⁶⁵ Anwarullah, *The Criminal Law of Islam*, 174-175.

⁶⁶ Sonny Zulhuda, and Sidi Mohamed Mohamed Ould. "The Shari'ah Approach to Criminalise Identity Theft," *Pertanika Journal of Social Science and Humanities* 23 (October): 169. ResearchGate, via ResearchGate, <https://www.researchgate.net/publication/316524215>.

⁶⁷ Rudolph Peters, *Crime and Punishment in Islamic Law, Theory and Practice from the Sixteenth to the Twenty-first Century*, 53-56.

⁶⁸ Theft via the Internet and the Application of Hadd.

⁶⁹ Sonny, "The Shari'ah Approach to Criminalise Identity Theft", 172-178.

report from the individual affected or the data manager, as advised by legal experts Abu Hanifah and Imam Syafie. This method may also consider further "circumstantial evidence" to support the assertion. Thus, based on this interpretation, it is possible to apply the notion of Personal Data Breach to the Sariqah offence, categorized under the Hudud crimes.⁷⁰ In short, it is apparent that personal data breach action confronts Sariqah's components regarding information theft. Personal data is valuable, and the perpetrator could illegally obtain it through technological proceedings, as discussed. However, the problem regarding the *Shubhah* principle may obstruct the proof of the elements of personal data breach as established by the Sariqah offence.

ICL continuously offers support for criminal charges categorized as *Ta zir*, including offences not explicitly outlined in the Quran and Sunnah. It pertains to miscellaneous criminal offences outlined in the leading legal source. *Ta zir* is the rudimentary word representing "respect" and aid. The main goal of this policy is to restrict and discourage any limitations, whether related to religious beliefs or other prohibited behaviours, including additional criminal activities. Regarding the verses of the Holy Quran,

*"And God said: I am with you if you (but) establish regular prayers, practice regular charity, believe in my apostles, honour and assist ('azzartumuhum) them" (Al-Ma'idah, 5:12)*⁷¹

*"So it is those who believe in him, honour him, help ('azzaruhu) him, and follow the light which is sent down with him" (Al-A'raf, 7:157)*⁷²

⁷⁰ Rudolph Peters, *Crime and Punishment in Islamic Law, Theory and Practice from the Sixteenth to the Twenty-first Century*, 53-60.

⁷¹ Al-Ma'idah: 12.

⁷² Al-A'raf: 157.

*“So that you (O men) may believe in God and His apostle that you may assist (tu‘azziruhu) and honour him, and celebrate His praises morning and evening.” (Al-Fath, 48:9)*⁷³

The Ta zir categorizes two basic explanations, explicitly labeling the illegal act as a "Personal Data Breach."

1. *Ma'siyah* is an extra criminal offence derived from interpreting primary Islamic law sources under Shariah, even if it is not clearly stated in those sources.
2. *Maslahah* denotes illegal behaviour against the Public Interest concept.⁷⁴ This principle intends to demonstrate how authorities can utilize the Ta zir notion to fill gaps or implement additional measures in substantive legislation when addressing technical concerns.⁷⁵ Traffic sanctions under "Transportation Law" are enforced to promote the appropriate use of transport and avoid accidents resulting from negligence that may endanger other individuals in the transport sector. To assess the relevance of Ta zir in cybercrime, specific instances of conduct considered criminal under this offence, as specified in the Anti-Cybercrime Act⁷⁶, must be provided.

When analyzing the unique Sariqah offence within the "Hudud" category, it is argued that the application of the law may encounter challenges due to the core principle of Shubhah, which refers to rudimentary doubts. This can result in disqualification scenarios where the complete punishment under Hudud may not be effectively carried out. However, Ta zir is subject to the discretion of the *Qadi* (Islamic Judge) and the

⁷³ Al-Fath: 9.

⁷⁴ Yrd. Doç. Dr. Recep ÇİĞDEM, "Concept of Ta'zir (Discretionary Punishment) in Theory and in Practice", *k Üniversitesi Hukuk Fakültesi Dergisi*, (2004): 167–185., Degipark, via Degipark, <https://dergipark.org.tr/en/download/article-file/262605>.

⁷⁵ Topo Santoso, "Implementation of Islamic Criminal Law In Indonesia: Ta Zir punishment as a Solution?", *IUM Law Journal*, vol. 19 (2011): 123–148. Heinonline, via Heinonline, <<http://www.heinonline.org>>

⁷⁶ Kingdom of Saudi Arabia Anti-Cybercrime Law, (Act. No. A/90)(Reprint 2007) (2007).

alternative punishment. The primary challenges in enforcing the law of personal data breach are as follows:

1. The accurate and unambiguous identification of "Personal Data" to assess the specific value of "Property." As Imam Ahmad and Imam Abu Hanifah stated, the property value that could result in applying Hudud punishment must be greater than 3 Dirham or $\frac{1}{4}$ Dinar. (1 Dinar is approximately 4.457 grammes of gold). According to the hadith, hands are not amputated for sums below 10 dirhams.⁷⁷ While questioning witnesses and probing personal data breaches, it is anticipated that there may be instances where a substantial amount of personal data is lost. The UK Election Commission 2023⁷⁸ found that numerous persons have been impacted, with millions of personal data breached from the database. Accurately identifying the categories of personal data and evaluating their Value poses a significant challenge when adopting the evidence rule. This issue and weakness over the property's value will lead to uncertainty in implementing the legislation. If declared invalid, the Ta'zir Punishment will be applied under the principle of substitutional punishment.

Proving personal data breaches relies heavily on electronic evidence and Forensic Identity challenges, which can be a significant hurdle in establishing the illegality of cybercrime and achieving all required requirements. Investigating a cybercriminal's participation in cybercrime, especially in cases of a personal data breach, requires tracing data trafficking, data tracing, IP addresses, and other pertinent information. This is crucial when the cyber-criminal has taken advantage of an "anonymous" position to commit the intrusion.⁷⁹ Moreover, one of the optional

⁷⁷ Anwarullah, *The Criminal Law of Islam*.,174-180.

⁷⁸ Neil Ford, "List of Data Breaches and Cyber Attacks in 2023", It governance, 2023, December 5. <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023> (Accessed 15 April 2024).

⁷⁹ Sawatree, *The Law and Regulations about Computer Crimes and Cybercrimes*.,69-73.

elements requires the presence of an eyewitness, referred to as the *Shahada*, who must fulfil the conditions of *Sariqah* by giving testimony to two male eyewitnesses. The witness must possess skill and knowledge in computers and technology to fully comprehend and describe how the criminal carried out the cybercrime.⁸⁰ Most electronic evidence is classified as circumstantial evidence based on the elements of *Sariqah*. The UK faced the Forensic Identity Challenge in the legal case *Smith and Others v Talktalk Telecom Group Ltd.*⁸¹ This challenge failed to implement the "Unauthorised Access Notification" and identify losses of personal data. Later cases encountered the same issue and were not successful in their execution. The Forensic Identity Challenge and the Data Growth Expansion⁸² may significantly contribute to confusion in determining culpability for the Hudud-Sariqah Offence.

Conclusively, the personal data breach from an Islamic Perspective is categorized into two viewpoints:

1. personal data breaches should be classified as criminal offences under the Hudud-Sariqah⁸³ category.
2. personal data breaches should be classified as criminal offences under the Ta'zir crimes category⁸⁴, as demonstrated by the legal framework in Saudi Arabia,

⁸⁰ Rudolph Peters, *Crime and Punishment in Islamic Law, Theory and Practice from the Sixteenth to the Twenty-first Century*, 53-60.

⁸¹ *Unauthorized Access proceedings in United Kingdom. [Smith and Others v Talktalk Telecom Group Ltd [2022] 1 WLR 5213]* 2022 May 19, Page 17: "The current MPI claim is rejected, and I decline to authorize any amendments based on the arguments presented in the draft RAPOC. If the user provides me with clearer instructions on a data protection claim, I will reject the application to strike out the "unconfirmed breaches". Therefore, the RFI Application is still active. I propose that the parties come to an agreement regarding a schedule for additional submissions and evidence concerning the application and subsequent orders resulting from this judgment. The claimants are instructed to submit a Report on the Progress of the Case (RAPOC) regarding the Unconfirmed Breaches claim, to be reviewed during the upcoming hearing."

⁸² Xichen Zhang, "Data Breach: Analysis, Countermeasures and Challenges", 402-442.

⁸³ Theft via the Internet and the Application of Hadd.

⁸⁴ Sonny, "The Shari'ah Approach to Criminalise Identity Theft", 169-182.

which is governed by the Islamic Legal system through the "Anti-Cybercrime Law 2007⁸⁵" and "Personal Data Protection Law 2021."⁸⁶

The Shubhah principles focus on evaluating personal data value and the challenge of Forensic Identity. They emphasize the importance of electronic evidence. If disqualifying Sariqah occurs, the judge may impose substantial punishment under Ta zir through discretionary considerations. Hence, it is concluded that this cybercrime should be classified under the Ta zir category rather than Sariqah offences, especially when it closely resembles "Information Theft." Eventually, when considering the complex nature of personal data breach and two critical aspects of law enforcement, the Ta zir approach is more effective in addressing the loophole through specific legislative measures rather than analogies with primary criminal offences like Sariqah.⁸⁷

The research lacks an official Islamic judicial revision and a well-known "fatwa" on this topic. As society advances, technology and humanitarian efforts expand rapidly. Islamic scholars may need to increase their understanding of the subject. The Islamic scholar should provide a clear religious decision addressing personal data issues, including classifying cybercrimes. The cyber-criminal receives suitable punishment and goes through a fair legal process to improve and manage the Islamic legal system more effectively while assuring good care for the victim.

2.4 CONCLUSION

Given the circumstances and description, the studies of personal data breaches found that several incidents involve cybercrime conducted through computer misuse and computer crime in the majority operation. Moreover, outsiders usually select the multi-

⁸⁵ Kingdom of Saudi Arabia Anti-Cybercrime Law, (Act. No. A/90)(Reprint 2007) (2007).

⁸⁶ Saudi Arabia Personal Data Protection Law(Royal Decree No. M/19)(2021), (Reprint 2023).

⁸⁷ Santoso, "Implementation of Islamic Criminal Law In Indonesia: Ta Zir Punishment as a Solution?" ,146-148.

layer invasion to disrupt and disable the target's function and breach into the storage to earn priceless treasures such as personal data.⁸⁸ Furthermore, the operation includes the "Insider" as the internal personnel who already knows the authentication process and has committed the personal data breach. This research also found that this incident could cover the terms of "Accidental" or unintentional personal data breach by the cause of uncontrollable factors such as human and system error.⁸⁹

In terms of the hackers, they are bifurcated in three main categories of incidents which could be highlighted that these operations involve "Information Theft", which affects societies from many angles. Firstly, the social view of this incident caused untrustworthy feelings among the population, including clients who are the personal data owners, when faced with unsafe circumstances from this incident. Meanwhile, the entrepreneur and government sectors also lose their reputation and security from this invasion.⁹⁰ Secondly, from the information base background, this incident caused the upcoming connectivity cybercrimes, especially Identity Theft, Scammers, and phishing. The economic causes of the losses of financial interest from the connectivity cybercrime are the root cause of illegal personal data disclosure and affect many victims. Also, the prime challenges to suppression take place for authorities since these cybercrime operations have existed for many years.⁹¹ Thirdly, the legal issues could be highlighted,

⁸⁸ Hassanzadeh, Biddle, and Marsen, User Perception of Data Breaches.,374-376.

⁸⁹ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*.,380.

⁹⁰ Thailand National Cyber Security Agency, *The Summarisation Operation Report 2021-2022 by Thailand National Cyber Academy*, (Thailand National Cyber Security Agency official website: Thailand National Cyber Security Agency, 2022),<https://ncsa.or.th/home> (Accessed 15 April 2024)

⁹¹ Jakrapong Kangwansophon, "Offenses of Fraud: Study of Telephone Scam Cases (Call Centers Gang)", *Research and Development Journal Bansomdejchaopraya Rajabhat University*, vol. 1 (2022): 280–290. ThaiJo, via ThaiJo, www.thaijo.org. In brief, the disclose damages from online fraud suffered victim hundreds million baht. However, currently, if calculated with the unpublic report of total damages, it is approximately reaching billions bath from these circumstances.

such as the fact that only the Computer Crimes principle was incomprehensive⁹² in arranging this incident, and there was also the lacuna⁹³ in taking legal action against the Data Controller under the large-scale personal data breach circumstances.

From these three effects of a personal data breach, the personal data protection principle, especially the CIA (Information Security) principles, is regulated in specific legislation by both EUGDPR and Thailand's PDPA, which are the only amendments that address the "personal data breach" definition⁹⁴ and make particular measures of compliance and specific sanctions for the inclusive responsibility to fill the loopholes that the necessary to uphold the security and obligations of personal data owners shall applicable. Moreover, the CIA principles also expanded and addressed the CSA and cybersecurity matters. This rudimentary legislation addresses the measures of cyber threats that are harmful to critical information infrastructure (CII).⁹⁵ Several incidents will highlight this unit as the primary target for invasion, espionage, and sabotage of the system.

Moreover, based on Islamic perspective already implemented and interpreted directly under rudimentary principle addressed and developed in the specific context from privacy to information security.⁹⁶ Meanwhile, from the Buddhist perspective⁹⁷, several religious teachings and thoughts implicitly apply the privacy principle through

⁹² Sonny Zulhuda and Ridoan Karim, *Cyber Law in Malaysia : Principal and Practices*, (Malaysia: Sweet and Maxwell, 2024),374-376. The author emphasised that the Computer Crimes Act should be inclusive and upheld in revision for updates to confront the recent cybercrimes.

⁹³ Worapit , "The Analysis of the Implementation of the Computer-Related Crime Act B.E. 2550". The author provides the recommendation that Thailand's Computer Crimes Act should be upheld with major Act revisions.

⁹⁴ Government Gazette, Thailand Personal Data Protection Act 2019. (Volume.136) (Chapter 69 Gor). Section 37 (4)

⁹⁵ Government Gazette, Thailand Cybersecurity Act 2019. (Volume.136) (Chapter 69 Gor).Section 3

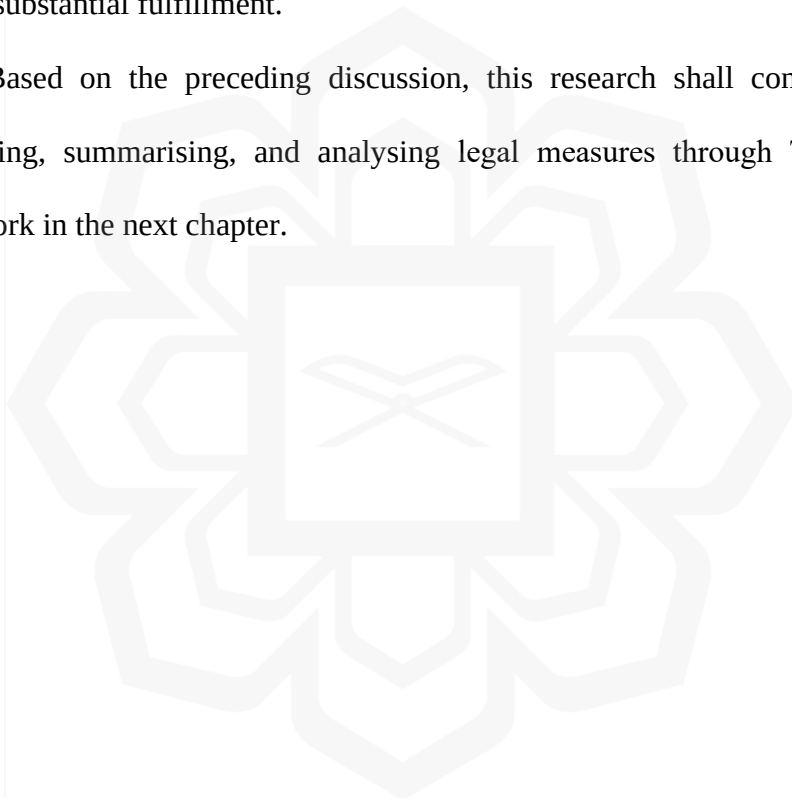
⁹⁶ Sonny, Information Security in the Islamic Perspective: The Principles and Practices.

⁹⁷ Sawaeng, *The Thai Legal History*.,49-55. From the main Thailand law development, which influenced from these codex's: 1. Three worlds of Phra Ruang (Sukhothai Era) 2. Thammasart and Rajsart doctrinal (Ayutthaya Era) and 3. The first law enactment (King Rama I of Rattakosin Era) still highlighted fundamental principles such as Theft, homicide, and Family Laws, but the illegitimate disclosure of secrecy was not explicitly mentioned in these referred doctrines.

isolation and mediating behaviour but were not directly implemented into the legislation as in Islam. Therefore, Thailand's legal amendments mainly implemented the legal principles of Western scholars as per Thailand's legal developments.

The previous explanation showed that various perspectives within the legal system, particularly the Islamic perspective and Islamic Criminal Law perspective, align with the general characteristics of personal data breach. As previously stated, the ICL demonstration still influenced the varying legal opinions and other options that needed substantial fulfillment.

Based on the preceding discussion, this research shall continue assessing, elaborating, summarising, and analysing legal measures through Thailand's legal framework in the next chapter.



CHAPTER THREE

ANALYSIS OF THAILAND’S LEGAL FRAMEWORK ON PERSONAL DATA BREACH

3.1 INTRODUCTION

The previous chapter discussed the characteristics, categories of operations, and primary causes of personal data breach in Thailand. Addressing legal redress may reveal that the initial stipulations of the Penal Code and CCC imposed several penalties to comply with punitive measures. In this regard, the general responsibilities of the legislature are tested beyond comprehension, with regard to imposing sanctions due to data breach.¹ Moreover, based on the rudimentary legislation, the central loophole was not regulated explicitly for personal data subjects, which should have been stipulated. Furthermore, CCA primarily encounters Information Communication Technology (ICT) systems misuse or original cybercrimes that make the ICT systems a tool prone to personal data breaches.² Therefore, the PDPA and CSA provisions specifically addressed the additional offences, including the necessary compliance duty, and provided the specific person applicable by the law as Data Subject, Controller, and Processor.³ This chapter demonstrated the overall Legal measures and the action to be taken in the circumstances of a personal data breach.

Generally, Thailand's legal framework amendments can be summarized into two main statutes, the Penal Code and the CCC, and three specific legislations, namely the

¹ Sarawut Pitayasak, *The Description of Thailand’s Computer Crimes Act First and the Second Edition (2007 and 2017)*, (Thailand: Nitithamlawbooks, 3rd edn., 2021), 60-79.

² Sonny Zulhuda and Ridoan Karim, *Cyber Law in Malaysia : Principal and Practices*, (Malaysia: Sweet and Maxwell, 2024), 298-307. Regarding the Information Communication Technology (ICT) system, terms will cover the original terms of “Computer system”. Personal data breaches not only damage “Computer Systems” but also harm other systems in cyberspace, such as cloud storage.

³ Government Gazette, Thailand Personal Data Protection Act. (Volume.136) (Chapter 69 Gor). Sections 3 and 4

CCA, CSA, and PDPA, which collectively provide precise measures to address situations regarding personal data breaches. Thailand's constitutional privacy and information status has been discussed and dealt with in sections 34 of the 1997 module and 35 of the 2007 edition of Thailand's Constitution. Constitutional law is sparingly applied to conflicts owing to statutory enforcement. The concepts of privacy are definitely constitutional, circumventing the "unconstitutional" approach to the law.⁴ Moreover, the legalization of the constitutional law impacted necessary Acts, including but not limited to the Official Information Act BE 2540 (1997)⁵, Trade Secret Act BE 2545 (2002)⁶, and Credit Information Business Act BE 2545 (2002)⁷.

However, these Acts indirectly addressed issues related to personal data because technology is devoid of a quantum leap in terms of unrestricted data flow. Under the purview of section 32 of the constitutional law of the Kingdom of Thailand, the promulgation of 2017⁸ explicitly regulated the term personal data in the national legislature as outlined in the primary statute. This implies that the idea of personal data protection has explicitly been addressed and acknowledged, as evidenced by the enforcement of the PDPA and CSA in 2019⁹.

⁴ Sneha Chawla, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments", (Unpublished Master's Independent Study Dissertation, Thammasart University, 2019), 20-25. The author emphasises that the actual practice in privacy matters is rarely. The public sector in Thailand is still developing administrative sections to address the upcoming legislation.

⁵ Government Gazette, Thailand Informations Act, (Volume 114) (Chapter 46 Gor)(1997).

⁶ Government Gazette, Act for the Establishment of and Procedure for Intellectual Property and International Trade Court, (Volume 139) (Chapter 32 Gor)(2015).

⁷ Sneha, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments". Page 55-60

⁸ Thailand's Constitutional. (Volume 114) (Chapter 40 Gor) (2017). Section 32 A person shall enjoy the rights of privacy, dignity, reputation and family. Any act violating or affecting the right of a person under paragraph one, or exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest.

⁹ Sneha, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments".55-60

The mission of Thailand's Constitutional Court involves bridging gaps between legal theory and practice, through interpreting and enactment of laws. Contemporary research exemplifies that privacy disputes related to constitutional problems remain devoid of promulgation.¹⁰ This assertion illustrates the significance of "mother statutes" in potentially amending the existing legislation in Thailand's legal system. The acknowledgement through constitutional law, significantly impacts Thailand's legal system through the specific provisions in the PDPA and the CSA, tantamount to address the pertinent issues related to personal data. This phenomenon signifies a paradigm-shift through interpretation of information into personal data and the cybersecurity framework, which, on the other hand strides in the earlier enforcement of CSA, enabling circumvention of cybercrime and data breach threats ineffective due to the lack of stipulated provisions from PDPA and CSA.¹¹ Eventually, even if the relevant enactments become effective, the rudimentary principle in Codes and the CCA are still relatively accessible in the application of each fact, through which the illegal action

¹⁰ Ibid. Based on the author's address of privacy issues, Thailand's judiciary rarely conducts legal exercises under the terms of Privacy. From this phenomenon, when the PDPA was addressed and enforced, many legal practitioners focused on this issue and intensely studied the legal measures between Privacy and Personal Data Protection principle inclusively.

¹¹ Bureau of Technology and Cybercrime, "The Research on the Effectiveness of Law Enforcement on Computer Crimes in the ASEAN Economic Community: A Case Study of Malaysia, the Republic of Singapore and the Republic of the Philippines". Department of Special Investigation Website, (Unpublished), 2021),, 1-4.

<https://www.dsi.go.th/th/Detail/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A8%E0%B8%B6%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%A7%E0%B8%B4%E0%B8%88%E0%B8%B1%E0%B8%A2%E0%B9%80%E0%B8%9E%E0%B8%B4%E0%B9%88%E0%B8%A1%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%AA%E0%B8%B4%E0%B8%97%E0%B8%98%E0%B8%B4%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9A%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%B1%E0%B8%9A%E0%B9%83%E0%B8%8A%E0%B9%89%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B9%80%E0%B8%81%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%A7%E0%B8%81%E0%B8%B1%E0%B8%9A%E0%B8%AD%E0%B8%B2%E0%B8%8A%E0%B8%8D%E0%B8%B2%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%84%E0%B8%AD%E0%B8%A1%E0%B8%9E%E0%B8%B4%E0%B8%A7%E0%B9%80%E0%B8%95%E0%B8%AD%E0%B8%A3%E0%B9%8C> (Accessed 10 March 2024).

shall qualify the components in each offence. This summarisation of Legal measures regarding personal data breach incident as follows;



Table 3.1 The summarisation of Thailand's legal measures in the event of a personal data breach (The substantive Legislation only)

The Statute	The objective of the Law	The person implicated by the law	Duties of the parties involved	Offense	Sanctions
Personal Data Protection Act 2019 (PDPA)	Arrange personal data breaches according to compliance rules, implement suitable cybersecurity measures, conduct the data protection impact assessment (DPIA), and notify relevant parties in case of a breach. Stakeholders are required to adhere to Personal Data Protection principles, including the CIA principles.	Data Subject, Data Controller, Data Processor	1. The Data Controller and Data Processor must comply with the law, particularly section 37 (1) and (4) of PDPA. The Data Processor is responsible for the obligations of the Data Controller and must adhere to sections 40 and 41 of PDPA. 2. The Data Subject has the right to file a complaint with the expert committee (PDPC) under section 73 for internal conflict resolution under PDPA or can directly take the issue to court under sections 77 to 83 of PDPA.	1. Any harmful and malicious behaviour or damages to the data subject may result in punitive compensation. 2. Data Controller's failure to comply and unauthorized disclosure of personal data, susceptible data. unauthorized release of personal data and its impact on performance. Moreover, these offences would be attributed to the legal entity as the offender. Non-compliance or violations by data controllers and data processors may be subject to assessment and inquiry by the PDPC expert committee.	1. Actual Damage compensation (section 77) and Punitive compensation (section 78) 2. Criminal Liabilities Section 79 to 81 3. Administrative Liabilities (Administrative Fine) in Section 82-90 (Highlighted on Non-compliance in Section 83)

Cybersecurity Act 2019 (CSA)	Specify the primary obligations of the "administrative agency" under the PDPA and provide the concept of "Cyberthreat." Furthermore, this legislation establishes the protocol and additional authority to address an emergency cyberattack.	Government Agencies, Cybersecurity Committee, Officer under the Cybersecurity Act.	Within the NCSC, NCRC (Cybersecurity Committee and the Organization), if an official commits Cybersecurity Liability Offences, the authority will be transferred immediately to the court or internal dispute resolution process, which may involve imposing administrative sanctions on the offender.	1. The Officer who violates this Act by unlawfully disclosing data or engaging in data trafficking, including intentional or negligent ICT system disruption. 2. Officer/Responsibility Organization Non-compliance under CRC and/or the Committee oversight. Addressing undisclosed emergency cyber danger and DPIA notification responsibilities. Furthermore, these offences will be attributed to the legal entity as the perpetrator.	1. Imprisonment and fines under the criminal liability section 70 to 72, 75 and 76 2. Administrative Fine under the Non-Compliance Liability section 72 to 74
Computer Crimes Act 2 nd Revision 2017 (CCA)	encounter the cyber danger, particularly the "Unauthorized Access" carried out by the perpetrators. The 2 nd version modifies the officer's exceptional authority under this Act, which will be activated promptly in case of an "emergency cyber threat."	-General Injured Person who is affected by a Personal Data Breach. -The Offender who commits the crime.	The injured person, whether an individual or a legal entity, should file a complaint with the police (Cyber Crime Investigation Bureau: CCIB) for investigation. The Prosecutor will then act as the plaintiff to pursue legal action against the offender in the criminal court (cybercrime division).	1. ICT system-related offences include Unauthorized access, sabotage of security systems, and common cybercrimes governed under Sections 5-12, with increased punishment explained in Section 13. 2. Regulation of malicious content (Sections 14-16)	Imprisonment and fines. Moreover, the punishment for these criminal liabilities shall increase if the offender's target is "Critical Information Infrastructure" under the provision in the 2 nd revision.

Penal Code	The general substantive offence is the primary law that applies to criminal offences.	- General Injured Person who is affected by a Personal Data Breach. -The Offender who commits the crime.	The Injured Person, whether a natural or juristic person, shall direct the complaint to the police (Cyber Crime Investigation Bureau: CCIB) to investigate and continue to proceed with the Prosecutor as the plaintiff to execute the offender at the criminal court (cybercrime division).	It depends on the specific case, especially the Non-Technical Personal Data Breach cases. Furthermore, Thailand possesses the identity theft criminal liability as interpreted in Sections 341 (Fraud) and 343 of Thailand's Penal Code.	Imprisonment and fines (depending on the specific provision)
Civil and Commercial Code (CCC)	The general substantive law lays down the general central principle for interpretation. The essential principle of Tort Law shall be applicable in the event of a Personal Data Breach regarding general compensation.	-The personal data breach affects the affected Person - The Offender who committed the crime. -The Data Controller and Data Processor are responsible for additional liabilities in providing compensation under this code.	The injured Person, whether a natural or juristic person, shall directly lawsuit the case to the court to the Data Controller/ Data Processor to request additional compensation. Moreover, this right might suit the offender and request compensation, too.	It depends on the case in which the plaintiff requests the court for determinations.	A judicial examination based on Section 438 CCC will determine the authority to grant compensation. Furthermore, the particular location might be the psychological damage compensation specified in section 446 that the wounded individual must seek in the event; this overarching rule is not eligible for compensation under Thailand's PDPA regulation.

Generally, Thailand's legal framework classifies divided the lead roles in personal data breach instances, through categorization into civil, criminal, and administrative liabilities. The rudimentary code serves as the backup, and CCA is the prescribed plausible solution, regulated to monitor ICT Systems misuse, as the PDPA and CSA play inclusive, albeit complimentary roles in the prevention, detection, and suppression measures regarding personal data breach circumstances. Emerging through this tentative explanation, the following section describes the role of the law regarding personal data breaches under each legislation.

3.2 PENAL CODE

According to the previous description of personal data breaches, the instances illustrated that these illegal activities are considered one of the categories of cybercrime. However, the rudimentary structures of the Penal Code and its overall criminal liabilities are implicitly prosecuted in the issues of the violation of personal data. Nevertheless, this Code is implemented precisely in the illegal revealing of confidentiality by the section's definitions. Section 322 of the Penal Code precise in encountering the unlawful reveal of secrecy of the perpetrator in this issue.¹²

“Section 322. Whoever, breaking open or taking away the closed letter, telegram or any document belonging to the other person so as to ascertain or to disclose its contents, if such act to be likely to cause injury to any person, shall be imprisoned not out of six months or fined not more of one thousand Baht, or both.”¹³

Unravelling records from the Supreme Court of Thailand, the research focuses on case number 253/2520 (1977), which is a typical case imparting Stare Decisis.

¹² Government Gazette, Thailand Penal Code. (Volume 139) (Chapter 28 Gor) (Revised 2022). Section 322. This section could demonstrate the rudimentary importance of confidentiality protection. However, this section of the Penal Code applies only to “Physical Privacy” but does not in terms of personal data violations due to the definition of personal data is not defined under the Penal Code.

¹³ Ibid.

During the proceedings of this case, the public prosecutor as a plaintiff, initiated legal action against the defendant for receiving a letter from one individual and subsequently transmitting it to another without obtaining prior consent from the grantor of the letter or any competent authority. The defendant pursued the declassification of the letter and disseminated its declassified sensitive contents publicly. The injured victims, who were dispatched and were bound to receive the letter reportedly claiming damages. Notwithstanding the defendant's repudiation of the allegations, the trial court imposed a sentence of one-month incarceration for the accused, who in the capacity of a defendant filed an appeal to the Supreme Court. The Supreme Court reversed the ruling and dismissed the appeal. As the appeal was submitted upon reaching the Supreme Court, it was ascertained that the offence in question was compoundable. The aggrieved individuals asserted that the parties had reached an agreement, through an out-of-court settlement with the defendant, to terminate the lawsuit. Thus, the dispute was resolved, and the Supreme Court, through the application of the legal conductance of Ratio Decidendi, approved/sustained the verdict from the Supreme Court to the Appellate Court.¹⁴

According to Chawla's study on criminal liability in violation of privacy, cases depict rare challenges over judicial decisions. Exercising judicial merits under the purview of the Penal Code primarily pertains to the sections concerning legal claims related to life/body and property-related offences. Section 322 clearly outlines the significance of criminal culpability, through the disclosure of confidential information

¹⁴ Court of Justice of Thailand, Thailand's Official Law Reports in Data Breach Case (Non-translation).<http://www.supremedekacourt.co.th> (Accessed 15 April 2024). In this case, the injured person, as the plaintiff, had negotiated with the defendant during appeal proceedings. This offence is the compoundable category in section 325 of the Penal Code. Thus, the parties could settle the dispute by negotiation when the result is agreeable to the parties, and the plaintiff could withdraw the lawsuit. The judiciary dismissed the case by agreeing with the plaintiff to withdraw the lawsuit as the result of section 325 of the Penal Code.

prone to harm the affected individual. This section suggests that it could apply to the "personal data breach" concept of the abuse of personal data, such as the unauthorized disclosure of confidential information, and violating confidentiality regulations. Section 322 of the Penal Code deals explicitly with the scope of disclosure through telegrams, letters, and papers, focusing on the legal implementation concerns related to personal data status loopholes.¹⁵

Contemporary research of the Thai legal system suggests enacted legislature through primary sources of law and legal statutes, leads to magnanimous discoveries, albeit the constitution already addressed the issues of personal data definition. Constitution upholds legal bindings enacted through promulgation of personal data in 2017. However, the courts shall apply the primary definition of "properties", as stipulated through Sections 137 and 138 of CCC.¹⁶ In case number 887/2501 (1958), the defendant including but not limited to accomplices unlawfully entered the building and illegally connected to the utility supply. The public prosecutor charged the defendant with a cognizable offense of "theft", offence under sections 334 and 335 of the Penal Code. Through the study of the General Meeting resolutions, the Supreme Court determined that the defendant committed theft by illegally consuming electricity.

However, the primary disqualification of over ridding the stipulated section, and components is due to a lack of compatibility of general provisions. The general characteristics needing to be consistent with the existing legal definitions, as electricity

¹⁵ Sneha, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments",55-60. From the previous discussion, it was found that Constitutional law section 32 regulated into specifically applied in the PDPA 2019. However, based on the Penal Code still does not apply the definition of personal data. Instead, the Penal Code application focuses on the definition of "Property".

¹⁶ Government Gazette, Thailand Civil and Commercial Code.(Volume 141) (Chapter 58 Gor) (Revised 2024). "Section 137. Things are corporeal objects. And Section 138. Property includes things and incorporeal objects that are susceptible to having a value and being appropriated."

can be considered a distinctive form and can be owned by individuals. Nevertheless, there is still insufficient evidence to corroborate the defendant's guilt. Therefore, the outcome of this case was nullified through legal proceedings. Legal scholars argued and were split into viewpoints regarding whether electricity, as a lead utility, should be considered as real estate/property based on the official case ruling. According to Thailand's CCC and Penal Code definitions, this electricity will not befall or does not qualify as real estate or property. The law differentiates it as property-related, particularly concerning "electricity, information, and personal data".¹⁷

In the case that followed 5161/2547 (2003), the court decided that the defendant accessed the data stored in the victim's ICT systems database, replicating it as a CD-ROM. The Supreme Court ruled that the information is considered unique under the purview of Section 137 of the CCC. The primary point is that "information" is distinct, a fact, and unchangeable. The graphics, arranged alphabetically, represent the main symbols, representing the morphology upon which information technology symbols are based, conveying information through the CD-ROM and ICT Systems equipment but cannot be accessed or transmitted. Thus, through the annals of the doctrine of precedent, the information is not a tangible property, and the act in question cannot be charged as Theft under the purview of section 334 of the Penal Code. The case was disqualified due to the components not meeting the requirements of the provision and was ultimately dismissed.¹⁸

¹⁷ Thailand's Official Law Reports in Data Breach Case (Non-translation). "Section 334. Theft. Whoever dishonestly takes away any property of another person or which the other person to be co-owner to be said to commit the theft, shall be imprisoned not out of three years and fined not more of six thousand Baht."

¹⁸ Sarawut , *The Description of Thailand's Computer Crimes Act First and the Second Edition (2007 and 2017)*,47.

According to the official law report number 12328/2558 (2015), employing the legal doctrine of obiter dictum, the judge procured the substantial legal decision, as it was overturned due to the defendants and coordinators' unauthorized utilization of public electricity for personal gains. The corroborative evidence submitted by the Metropolitan Electricity Authority, as the plaintiff, demonstrated the recognition of the debt agreement between the plaintiff and the defendant, highlighting the defendants culpability in the theft offence for the court's consideration. Consequently, the court's review of the comprehensive evidence, including but not limited to documentary materials, determined that the utility fee losses are substantial amounting to Thai Bhat Eight Million, Nine hundred and Sixty Seven Thousand, Two Hundred and Seventy decimal zero eight Only (THB 8,967,270.08/-), and it is inferred that the defendants perpetrated the crime. The defendants are liable under section 335 (7) of the Penal Code and remit compensation payments as proven through corroborative evidence under section 29.¹⁹

These three significant cases covered under the Penal Code demonstrate the Code's interpretation and implementation regarding criminal liability for property-related offences. However, the Penal Code remains the major lacuna problem in interpretation and implementation precisely on the subject of personal data. This Code concerning cybercrime focuses on addressing and combating crimes under "Identity Theft" and illegal operations on physical activities. In short, the primary criminal

¹⁹ Thailand's Official Law Reports in Data Breach Case (Non-translation). "Section 335 Whoever commits theft under any of the following circumstances: By carrying arms, or by having two persons upwards participating. Shall be punished with imprisonment of one to five years and fined of two thousand to ten thousand Baht. If the offence committed according to the first paragraph comes under the circumstances provided in the above-mentioned sub-sections from two sub-sections upwards also, the offender shall be punished with imprisonment of one to seven years and fined of two thousand to fourteen thousand Baht."

offence under the Penal Code was Fraud under an enactment of Section 341, with the penalty for deception related to fraud as a cognizable offence under Section 343²⁰.

Case numbers 831/2559 (2016) and 79/2564 (2021)²¹ are examples of law applications under the Penal Code where cybercriminals illegally obtained personal data from databases and abused the data blatantly through online fraud offences. The prominent suppression against cybercrime in Thailand will focus on this illegal action (Online Fraud) from 2019 until the present. Moreover, legal practitioners still adhere to the law application through the Penal Code. Therefore, from 2019 to 2022, personal data breach seem to be overlooked due to the intense suppression by legal practitioners and authorities.

Conclusively, the principal criminal offence, as applied under the purview of the Penal Code, could potentially be applicable to the additional offence connected with the personal data breach. The scope covers 1. The offender who breaks the law, and 2. The officer, under the Penal Code's definition, is liable under the officer's liabilities. Specifically, the personal data will be preserved in documented form, including paper files, and stored in physical forms. These unlawful operations will be liable to prosecution under the Penal Code.

In conclusion, the Penal Code stipulates the additional criminal liabilities regarding personal data breaches by establishing liability for crimes under specified conditions as follows;

²⁰ Government Gazette, Thailand Penal Code.(Volume 139) (Chapter 28 Gor) (Revised 2022), Section 341 -343

²¹ Jakrapong Kangwansophon. "Offenses of Fraud : Study of Telephone Scam Cases (Call Centers Gang).", *Research and Development Journal Bansomdejchaopraya Rajabhat University*, vol. 1 (2022): 280–290. ThaiJo, via ThaiJo, <http://www.thaijo.org>. The illustration of the recent Penal Code application against Online Fraud, which is the continuous consequence of personal data breaches as illegal personal data usage activities. However, the precise operation of personal data breach is not emphasised in the suppression of the Call-Center Gang or Online Fraud.

1. The unlawful disclosure of confidential information, as provided in sections 324 and 323.

2. The officer unlawfully revealed the organization's classified information illegally under sections 161-164.²² Regarding public officer's liability, prior to the implementation of the PDPA, both citizens and legal practitioners were oblivious to the risks associated with Information Security principles, as demonstrated by the offence of unauthorized disclosure stemming from confidentiality breaches.

3. The unlawful liability under "property-related crimes" focuses on the physical activity of illegal action, such as theft offences under sections 334 and 335 and Fraud under sections 341- 343 of the Penal Code.

This research indicates that specific criminal offences impose criminal liability in Thailand, as further elucidated in the CCA, CSA, and PDPA.

3.3 CIVIL AND COMMERCIAL CODE (CCC)

Initially, the general definition of the provision is provided in Sections 420 and 421 of Thailand's CCC.²³ These provisions could be included in civil (tort) and criminal law to seek damages for financial harm caused by unlawful conduct to an individual. The connection between the tort compensation request and the criminal suit for the sanction can be linked through section 44/1 of the Criminal Procedure Code (CRPC).²⁴ Civil

²² Government Gazette, Thailand Penal Code. (Volume 139) (Chapter 28 Gor) (Revised 2022). Section 161-164

²³ Government Gazette, Thailand Civil and Commercial Code. (Volume 141) (Chapter 58 Gor) (Revised 2024). "Section 420. A person who, willfully or negligently, unlawfully injures the life, body, health, liberty, property or any right of another person is said to commit a wrongful act and is bound to make compensation." "Section 421. The exercise of a right which can only have the purpose of causing injury to another person is unlawful".

²⁴ Government Gazette, Thailand's Criminal Procedure Code, (1934).(Volume 136) (Chapter 34 Gor) (Revised 2019), Section 44/1 As for a public prosecution, if the victim is entitled to claim compensation in as much as the commission of offence by the defendant has caused him to lose his life, or sustain bodily or mental harm, personal liberty injury, reputation impairment or proprietary damage, he may submit to

liability and criminal sanctions related to personal data breaches in cybercrime cases may involve offences such as identity theft or online fraud. Cybercrimes often involve obtaining information vis-a-vis personal data breach and coercing the victim to send money illegally.

Sections 420 and 421 of the CCC lay down the main principles of “Liability based on fault”, in which the plaintiff shall bear the burden of proof for the components of the legal maxim under the standard of proof mentioned in Section 84/1 of the Civil Procedure Code (CPC).²⁵ Nevertheless, the standard of proof in the tort case is different from the standard of evidence proof in the criminal case under the purview of the Penal Code. The standard of proof beyond a reasonable doubt is in section 227, paragraph 2 of the CRPC.²⁶ Meanwhile, the standard operating procedures adopted under the auspices of the Tort law principles require that they be conducted under the “proof on a balance of probability” standard or following the standard of proof as stipulated in CPC section 104.²⁷

To illustrate, the plaintiff filed the lawsuit against the defendant under a general tort case under section 420 of Thailand’s CCC, in which the plaintiff shall prove the following components of the substantive principles:

1. Damage occurred by the wrongful actions.
2. It is caused due to by intention or negligence.

the court trying the criminal case a motion for coercively directing the defendant to make compensation for such loss.

The motion under paragraph 1 must be submitted before the taking of evidence takes place or, where the taking of evidence is not required, before the case is adjudicated. Such motion shall be deemed as a plaint under the provisions of the Civil Procedure Code, and the victim, the plaintiff. In this respect, the motion must contain reasonable particulars as to the loss and the amount of compensation claimed. Viewing that any gravamen in the motion is inadequate, the court may order the movant to correct the motion.

²⁵ Government Gazette, Thailand Civil Procedure Code.(Volume 134) (Chapter 69 Gor) (Revised 2017).

²⁶ Government Gazette, Thailand’s Criminal Procedure Code. (Volume 136) (Chapter 34 Gor) (Revised 2019), Section 227, paragraph 2

²⁷ Government Gazette, Thailand Civil Procedure Code.(Volume 134) (Chapter 69 Gor) (Revised 2017). Section 104

3. It has causality (the relationship between cause and effect) between the activity and the damage.

4. Compensations will be awarded to the plaintiff by the defendant through the courts.

If the plaintiff can not establish these facts, the court may not provide the remedies and compensation, or the case may be dismissed.

Another category of baseline civil liability in legal provision is “strict liability” or “liability based on fault.” The characteristics of this liability are slightly different from those of previous liability because this offence is based on the regulated legal provision and strictly follows the components of legal statute. The personal data breach is considered an illegal action based on the provisions of general tort law principles in Thailand’s legal framework in the context of providing “compensations” for repaying the harmful and any damages from unlawful actions. The CCC principles could illustrate the primary basis of compensation categories, which could determine and evaluate the appropriate compensation that provides the basis of compensation as follows :

1. Material Damages (Actual Damages) generally pertain to financial compensation. The loss can be quantified in terms of monetary value, such as expenses related to healthcare, lost income, and other costs resulting from the accident.²⁸ Assessing the damage might be complex due to the lengthy process of determining the extent of the damage. Material damage is not just what has occurred and exists but also encompasses force majeure, including what will inevitably occur. If someone's body is damaged, they must be treated at the hospital. The damage will be closely related to the incident.

²⁸ Theerachit Jitkarunawong, “Civil Liability under Data Protection Law: A Comparative Study of Thailand’s Personal Data Protection Act And EU’s General Data Protection Regulation (EUGDPR)”, (Unpublished Master's. Independent Study Dissertation, Thammasart University, 2019).

2. Compensations are awarded based on non-material damages, which face the challenges of determination and evaluation. The injured individual may experience material and non-material losses, including pain, suffering, and loss of amenities. In Thailand, non-material damage is not explicitly outlined in the CCC. However, it typically manifests in the plaintiff's demand for damages through grief, melancholy, solitude, and disappointment. The legislation does not define non-material damage to avoid complicating the burden of proof for damages and to limit the court's discretion. The Supreme Court shall grant compensation for non-material damage if the plaintiff can demonstrate the presence of non-material harm as outlined in Section 446 of the CCC.²⁹

If only non-material damage is filed as a claim, the Supreme Court might not decide in favour of the petitioner. Moreover, intangible harm must directly result from the claimant's injury. If the damage is solely indirect, such as a husband unable to obtain compensation for emotional pain stemming from the loss of his wife, who brought them joy, due to the activities of an individual who did not violate the law. The husband possesses no legal grounds for a lawsuit, as established by the general interpretation and application in case number 789/2502 (1959)³⁰. Another notable case related to immaterial damages is case number 4571/2556 (2013).³¹ The Supreme Court later granted modest damages to the plaintiff in a specific case. The defendant did not fire the gun but used one to threaten the plaintiff, causing harm to the plaintiff's health and

²⁹ Government Gazette, Thailand Civil and Commercial Code.(Volume 141) (Chapter 58 Gor) (Revised 2024). ” Section 446. In the case of injury to the body or health of another or the case of deprivation of liberty, the injured person may also claim compensation for the damage, which is not pecuniary loss. The claim is not transferable and does not pass to the heirs unless it has been acknowledged by contract, or on action on it has been commenced.”

³⁰ Thailand's Official Law Reports in Data Breach Case (Non-translation).

³¹ Ibid.

well-being. This resulted in psychological harm and was classified as non-material damage under Section 446 of the CCC. Therefore, the plaintiff has the right to pursue for compensation in this circumstance. The categories of damages will be used in the standard determination clause of Section 438 in CCC.³²

The CCC principles examine privacy infringement under general tort principles to determine whether Information Security principles are rarely implemented. Official law decisions can be observed in Thailand's Supreme Court case number 4893/2558 (2015). The defendants, an editor, and a publishing company published a news article alleging that the plaintiff had engaged in sexual activity with his partner. Other news sources covered this information while maintaining the plaintiff's anonymity. The defendants revealed the news and verified that the photograph identified the plaintiff. The plaintiff happened to be a politician with a public image. The plaintiff's privacy was violated according to section 420 of the Civil and Commercial Code. Submitting a complaint and providing details of the violation does not mean the plaintiff consented to their identity being revealed to the public. Despite being famous, the plaintiff still has the right to privacy. The media defendants have the right to freedom of expression, which does not justify violating someone's privacy. The defendant was found to have violated section 420 of the Civil and Commercial Code.³³

Further review of personal data breach occurrences and the ramifications of PDPA principles impact CCC in its support function as additional compensation. Furthermore, the PDPA primarily implemented strict liability, encompassing the

³² Government Gazette, Thailand Civil and Commercial Code.(Volume 141) (Chapter 58 Gor) (Revised 2024). "Section 438 of the CCC: The court shall determine the manner and the extent of the compensation according to the circumstances and the gravity of the wrongful act. However, compensation may include restitution of the property the injured person has been wrongfully deprived of or its value and damages for any injury caused."

³³ Thailand's Official Law Reports in Data Breach Case (Non-translation).

rationale for liability exemption inside the law. Consequently, CCC will seek supplementary compensation based on the Data Controller's payment of remedies in accordance with PDPA principles.³⁴In the context of an offender who committed a personal data breach and was sued by the Data Controller or Injured person, CCC will be applicable as the rudimentary law.³⁵This basis could illustrate the damages caused by the invasion to injure a person and the victim's institution. The damage could be calculable from personal data misuse, and the losses of recovery after the invasion could be included under a strict liability basis.

The principle of civil liability under the PDPA is based on strict liability. Section 78 of PDPA imposes punitive sanctions on Data Controllers and Data Processors who are found to be negligent in allowing personal data breaches to occur. The punitive sanction can be raised up to two times the compensation determined under section 77, enables Data Subjects to prove damages with supporting documents. The court employs its prerogative to offer legal redress, through stare decisis, based on the authority granted by the statute.

However, under the legal practices of tort law principles will rely on a "liability base without fault" basis to ensure the provision of remedies and the submission of evidence necessary for compensation assessment. Non-material damages should address personal data breach issues to provide comprehensive remedies, particularly for individuals who may experience fear or mental health conditions necessitating essential treatment. The organization suffers a decline in reputation and potential business opportunities due to diminished trustworthiness resulting from breaches in internal

³⁴ Theerachit, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act and EU's General Data Protection Regulation (EUGDPR)".44.

³⁵ Government Gazette, Thailand Civil and Commercial Code.(Volume 141) (Chapter 58 Gor) (Revised 2024). Section 420. Meanwhile, in the PDPA framework, the main parties are the Data Subject and Data Controller/ Processors.

security. The samples could not be assessed based on actual damage due to the inability to evaluate the personal data breach incident comprehensively. Additionally, non-material damage under section 446 of CCC, pertaining to "Liability based on fault," necessitated that the party assume the burden of proof for the damage incurred.³⁶ The possibility of granting remedies less than "strict liability" is based on the obstruction in the "burden of proof." It is recommended that this issue regarding non-material damage in personal data breach incidents should be addressed in further studies.³⁷

In conclusion, the judiciary plays a crucial role in the country's legal system by guiding the interpretation and application of laws. The general tort law principle regulates civil liability when a cybercriminal, accountable for a personal data breach, and a Data Controller/Processor do not adhere to specific provisions and may have either intended or been negligent in inflicting harm or damages on the affected individual (Data Subject). The general tort law provision establishes a legal framework that governs the obligations of the injured person (Data Subject), the subject of the law acting as Data Controller/Processor, the Data Controller/Processor, and the perpetrators who conducted the illegal actions, contingent upon the context of a lawsuit. The central challenge of the CCC application is the burden of proof.³⁸ This requires each plaintiff to find reliable evidence to prove damages related to personal data breach matters to receive appropriate court remedies. The principles may not fully address all the harms of personal data breaches. The closest relevant legislation to address civil liability issues

³⁶ Ibid. Section 446

³⁷ Theerachit, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act and EU's General Data Protection Regulation (EUGDPR)". It is agrees with the author's suggestion to put this non-material damages issue into further in-depth study. Furthermore, this study addressed the obstruction of proof of the damages from personal data breaches, especially the losses of reputation from data breach incidents, which makes it difficult to obtain compensation from the court.,53-55.

³⁸ Government Gazette, Thailand Civil Procedure Code.(Volume 134) (Chapter 69 Gor) (Revised 2017).

is Thailand's PDPA, which will be further discussed in the PDPA section. Also, the criminal liabilities under the “ICT-related crime” will be described in the next section.

3.4 COMPUTER CRIMES ACT (CCA) (2007)

The previous section indicates that cases examined judicially regarding the concepts of "electricity" and "information" under the Penal Code shed light on Thailand's lack of familiarity with new types of criminal activities during the 2000s, leading to challenges in legal interpretation. Thailand implemented and provided the initial version of the Computer Crimes Act 2007, and the legal technique was then transplanted as stated. After the enforcement of the CCA, crime categories were expressly divided into ICT systems-related crimes, as outlined in the Convention on Cybercrime.³⁹ The main computer crime illegal access offences which involve personal data breaches are as laid down in the sections 5 and 7 of CCA;

“Section 5 Whoever illegally accesses to a computer system that has specific security measures and such security measures are not intended for his/her use, shall be liable to an imprisonment for a term not exceeding six months, or a fine not exceeding TenThousand Baht or both.”⁴⁰

“Section 7 Whoever illegally accesses to a computer data that has specific security measures which are not intended for his/her use, shall be liable to an imprisonment for a term not exceeding two years, or a fine not exceeding Forty Thousand Baht or both.”⁴¹

The previous section of the study showed the cases analysed under the Penal Code were prior to the implementation of the CCA's first edition and the 2015 case. This period marked Thailand's judiciary's focus on societal progress and evidence

³⁹ Council of Europe, “Council of Europe Convention on Cybercrime, Budapest, 2001,” <https://www.coe.int/en/web/cybercrime/the-budapest-convention>. (Accessed 15 April 2024)

⁴⁰ Government Gazette, Thailand Computer Crimes Act 2007, (Volume 124) (Chapter 27 Gor) (Revised 2017).

⁴¹ Ibid.

improvement to reach case outcomes. The main role of substantive legislation in combating cybercrime in Thailand involves transitioning from the pre-enforcement of the CSA and PDPA to the post-enforcement of the CCA to punishing cyber criminals under the sanctions of the Act.⁴² During the drafting process of the initial enforcement, this Act underwent a more extensive examination and evaluation in Parliament before being passed and enforced due to the unique nature of cybercrime and computer crime and the simultaneous passing of numerous Information and Technology legislations. Thus, Thailand needs to catch up to implement this Act.⁴³

Eventually, the Computer Crimes Act began to impact society by addressing "ICT-related" offences, technological advancements, and emerging issues relating to personal data protection. Illicit activities across the spectrum of cyberspace have risen, as discussed above. The political situation changed when General Prayut Chan-O-Cha became prime minister and created a new ministry called the Ministry of Digital Economy and Society (MDES) from 2015 to 2019. The parliament resolved to conduct a second revision of the CCA in 2017. Thailand has experienced a high number of cybercrimes and personal data breaches.⁴⁴ The second revision appears to concentrate on the issue of the online deferment interpretation, which coincided with the Penal Code and the approaching "Call-Centre Gang" following the AIS crisis from 2018 to 2020. The second revision of the CCA has another concern that impacts the efficiency of legal procedures in dealing with personal data breach issues within the context of criminal sanctions.

⁴² Sarawut, *The Description of Thailand's Computer Crimes Act First and the Second Edition (2007 and 2017)*, 27-31.

⁴³ Suneti Kongthep, *Demonstrations of Thailand's Computer Crimes Act*, (Thailand: Krungsiam Publishing 2015), 20-30.

⁴⁴ Sarawut, *The Description of Thailand's Computer Crimes Act First and the Second Edition (2007 and 2017)*, 26-31.

The reformation under CCA shifted supervision from the IT 2000 institution in the information technology forum to the Ministry of Digital Economy and Society (MDES) establishment due to political changes. The government (Gen. Prayut) established DE by virtue of Section 4 of Thailand's CCA 2nd revision.⁴⁵ It might be inferred that Thailand's legislators were informed about the EUGDPR initiative in 2015. The reform of CCA is necessary for the supervising ministry to implement and examine any subordinate or secondary regulations to address gaps in legal interpretation.⁴⁶

Furthermore, the reason for the major revision of CCA found the interpretation between The Penal Code and CCA regarding new categories of cybercrimes which are online defamation, spam, and phishing, which are considered as actual crimes on the internet or cyberspace. Primarily, these illegal activities are linked to rudimentary offences under the Penal Code sections 326, 328, 341, and 343, causing direct financial harm to the victim.

Significantly, the CCA second revision provides the increasing punishment reasoning from sections 5 to 11 of CCA by adding another section of 12/1 and 13 paragraphs 2 to 5 that if these ICT systems-related offences conducted by the target as the public infrastructure as occurred as; *“harmful to national cybersecurity organization or public infrastructure shall be punished....”* And *“If this computer-related offence in sections 9 and 10 causes the injured person to death, the offender shall be subject under section 200 of Penal code by analogy interpretation”*.⁴⁷

⁴⁵ Ibid.

⁴⁶ Ibid., 26-35 also CCA sections 11 and 12 on 2nd revision.

⁴⁷ Ibid., 26-35 included the additional document in the appendix

From the CCA revision, it could be considered that the “CCA has adopted the principles to confront the upcoming enactments, especially CSA.”⁴⁸ CCA was earlier adopted and the principles confronted with the other two primary legislations were fully implemented. The revision in section 2 of the Computer Crimes Act 2017 focuses on reformation related to the "Computer Crimes Act officer," specifically the Police authorities responsible for cybercrime. It includes revising their powers, duties, fees, and payments for cybercrime investigations and operations. The "Competent Officials section.”⁴⁹ The amendment could establish the centralization of Thailand's administrative structures from the Ministry of Supervision (MDES), specific authorities (under the NCSA authority), and distinctive functions linked to ICT systems related to criminal offences.

Furthermore, relevant doctrinal research should be conducted on the operational efficacy, overlapping issues, and the role of CCA officers in Section 2 of the CCA.⁵⁰ Post the amendment of the CCA, Thailand's government sectors and the Ministry of Digital and Economy established the CCIB, which is separate from the "Department of Special Investigations.”⁵¹ and plays a significant role in the "9 Near" operation.

Thailand's Computer Crimes Act was essential in capturing and prosecuting the perpetrator responsible for a personal data breach using specialized terms that deviated

⁴⁸ Ibid. The author attached the Government Gazette of the official Thailand CCA draft to refer to in the Book's Appendix. CCA 2nd revision had increasing punishment when computer crimes invaded CII (critical infrastructure units), which CSA also recognized and provided synchronized measures.

⁴⁹ Government Gazette, Thailand Computer Crime Act 2nd revision. (Volume 124) (Chapter 27 Gor) (Revised 2017). Section 18 and Section 19

⁵⁰ Sarawut, *The Description of Thailand's Computer Crimes Act First and the Second Edition (2007 and 2017)*.

⁵¹ Thailand National Cyber Security Agency, The summarisation operation report 2021-2022 by Thailand National Cyber Academy, Thailand National Cyber Academy official website. (2022), 1-5. https://ncsa.or.th/Ebook_%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%88%E0%B8%B3%E0%B8%9B%E0%B8%B5%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A%202566.html (Accessed 15 April 2024)

from the guidelines of the Penal Code. The second version of CCA does not address the core issue of criminal liability in the "Computer-related offences" section, resulting in a problematic situation.⁵² Furthermore, previous studies have noted that the revision of criminal liability in the context of cybercrime is not fully comprehensive in addressing the complicated nature of cybercrime. They suggest that a rudimentary revision and reformation under criminal liability should use the term cybercrime instead of computer-related offences, aligning with the focus of the Convention on Cybercrime, which emphasizes crimes committed using ICT and those aimed at sabotaging ICT systems. This could impact Thailand's interpretation of "Computer-Related Crime" legislation. However, according to the rules of the CCA, the primary criminal liabilities for engaging with the offender are unauthorized access offences.⁵³

According to the CCA's criminal liability, it could be demonstrated that the provision was selected using the word Illegal Access, which was adopted and adjusted from "Unauthorized Access" from the Convention. However, from the distinctive point of a personal data breach, the main first layer of illicit action is precisely liable for illegal access by nature. It is considered that the current personal data breach operation has become more complicated in the operation processing, such as the illegal access combined with ransomware, including the DDOS, into disrupted victim's functioning as mentioned in chapter two. Therefore, CCA 2017 faced the new challenges of new categories of cybercrime in which only illegal access offences might not be comprehensive in terms of law implementation.

⁵² Government Gazette, Thailand Computer Crimes Act 2007.(Volume 124) (Chapter 27 Gor) (Revised 2017).

⁵³ Government Gazette, Thailand Computer Crime Act 2nd revision. (Volume 124) (Chapter 27 Gor) (Revised 2017). Sections 5 and 7, as mentioned.

As mentioned above, the practical cases under the CCA applied illustrate that even though the case occurred prior to the full enforcement of the CSA and the PDPA, it was still in the drafting process. Nevertheless, these samples of official law report cases illustrate that Thailand's legal framework has the significance of succession in the procedure and has brought the perpetrator to be punished under the criminal sanction of CCA.

Primarily, Case number 3473/2563 (2020) pertains to the alleged occurrence of illegal access in Thailand's public hospital. The witness testimony in court shows that the defendant permitted access and used a DDOS attack to disrupt the target system's operation. The court's discretionary analysis and interpretation of the legislation suggest that the defendant's illegal access and DDOS attack actions could result in different kinds of punishment as outlined in sections 5, 7, and 9 of the CCA.⁵⁴ The public hospital is also considered the "Public infrastructure" liable under Section 12 (first version) and Section 10.⁵⁵ The judge's conclusion may be influenced by the continuous evolution of the public hospital's internal ICT and connection system. Afterwards, the technical

⁵⁴ Government Gazette, Thailand Computer Crimes Act 2007.(Volume 124) (Chapter 27 Gor) (Revised 2017). "Section 9 Whoever illegally acts in a manner that causes damage, impairment, deletion, alteration or addition either in whole or in part of computer data of another person, shall be liable to an imprisonment for a term not exceeding five years, or a fine not exceeding One Hundred Thousand Baht or both."

⁵⁵ Government Gazette, Thailand Computer Crime Act 2nd revision.(Volume 124) (Chapter 27 Gor) (Revised 2017)." Section 12 In case the perpetration of an offence under Section 5, Section 6, Section 7, Section 8 or Section 11 is associated with computer data or the computer system(s) that relates to the national security and safety, the public security, the economic security of the Kingdom of Thailand, or the basic infrastructure for the public interest, the offender shall be liable to an imprisonment for a term of one year to seven years, or a fine of Twenty Thousand Baht to One Hundred Forty Thousand Baht or both.

In case the perpetration of the offence under Paragraph 1 causes damage to such computer data or computer system, the offender shall be liable to an imprisonment for a term of one year to ten years and a fine of Twenty Thousand Baht to Two Hundred Thousand Baht.

In case the perpetration of the offence under Section 9 or Section 10 is associated with computer data or computer system as specified in Paragraph 1, the offender shall be liable to an imprisonment for a term of three years to fifteen years and a fine of Sixty Thousand Baht to Three Hundred Thousand Baht."

specialists identified abnormal behaviour while installing new equipment and testing the new system.⁵⁶

Furthermore, this case report found that the defendant's identity is that of the technical officer in charge of implementing the new connectivity system and new features of the hospital's application. Moreover, the public prosecutor has gathered evidence indicating that the defendant intentionally breached the security system to obtain sensitive information from the hospital's database through illegal access. This motive was achieved by launching a DDOS attack, causing a temporary weakness in the hospital's system. The data collected during this process is electronic evidence that can be legally presented in court for examination. Eventually, the defendant was held responsible under the CCA. This case occurred prior to the implementation of the second revision of the CCA and the effective date of the CSA (2016-2018). The defendant will be held accountable under the initial version of CCA. This case exemplifies the application of CCA and Thailand's legal framework in addressing personal data breaches related to "illegal access" precisely and directly. Moreover, this scenario should be considered during the full implementation of the CSA and PDPA. It may involve examining the actual implementation of Thailand's legal framework.⁵⁷

Similarly, in the second case, 2600/2563 (2020), the defendant was an ex-employee of the injured person's company. While the defendant was still employed by the company, unauthorized access was made to the plaintiff's internal security system, and significant information was collected from the database system. The defendant was aware that the area was restricted and that only individuals permitted by the plaintiff could access the material. The defendant later uploaded substantial information to his

⁵⁶ Thailand's Official Law Reports in Data Breach Case (Non-translation).

⁵⁷ Ibid.

email and sent it to third persons. The defendant's actions met the conditions of the illegal access offence full of the elements and guilt under section 7 of the Computer Crimes Act by unlawfully accessing the plaintiff's limited database, despite the defendant's argument that the legal definition of terms should exempt the material. The interpretation of judicial from the definition concept in the Electronic Transaction Act 2001 (2544) and CCA 2007 has already acknowledged and dealt with the information problem. Hence, this argument was rejected, and the defendant received the sentence according to Illegal access offences under section 7 of Thailand's CCA.⁵⁸

In another case involving the illegal access offence under CCA 2017, the official law report may state that the facts of the case match those of the personal data breach. In case number 4480/2564 (2021), the plaintiff's company employed the defendant. Upon authorization from the plaintiff, the defendant could access and manage the internal system and its data from the plaintiff's client. The defendant ensured data integrity before resigning and leaving the plaintiff's organization. The plaintiff discovered that the defendant illegally accessed a restricted database system, capturing internal corporate information and client data totalling around 30,000 records. Moreover, the data trace extends to the defendant's email account and the IP address. The database system is considered a highly secure closed area, typically inaccessible to the defendant without specific permission. This information is the primary evidence for the plaintiff's argument in court. The court rejected the defendant's claim that the recorded personal data were only preserved for security purposes. The defendant was

⁵⁸ Ibid. The defendant accused that the “information” terms are unavailable in the CCA and the Penal Code. Therefore, this action shall not be liable as the plaintiff suited the case and the “information” that the defendant earned is not important or harmful to the company. However, the Electronic Transaction Act of 2004 defined the “information” as being transmitted through the system, including the “data” transmission through the computer (ICT) system. Therefore, the defendant's action of accessing the restricted area without authorisation and earning the information sent to the third parties fills the components of CCA criminal offence.

guilty under the illegal access offence and sentenced under sections 5 and 7 of Thailand's Criminal Code Act.⁵⁹

In conclusion, the Computer Crime Act (CCA) is the primary legislation to address personal data breaches related to "Computer-Related Crime: Illegal Access." Furthermore, the operation's success in addressing the difficulty of "Forensic Identity" in electronic evidence can be seen in real sample practice cases due to the distinct power authority in section 2 of CCA and the emergence of Thailand's CCIB. The individuals most likely to be detected in Thailand are skilled in technological knowledge and proficient at exploiting loopholes to access victim databases. The study confronts the earlier analysis of personal data breach characteristics and suggests further examination of the cybercriminal realm in Thailand.⁶⁰ The discussion above indicates that the CCA 2nd version primarily focuses on criminal responsibility for cybercrime and may not address solutions for preventing and treating the victims.⁶¹ The following section will provide detailed information on the legal regulations of Thailand's CSA and PDPA.

3.5 CYBERSECURITY ACT 2019 (CSA)

The tentative mention of the role in the CSA unravelled the definition of this Act is recognising the "Critical Information Infrastructure" (CII) unit⁶². The main effect of the legal deficiencies of this unit was identified regarding the necessary and specialized

⁵⁹ Government Gazette, Thailand Personal Data Protection Act 2019. (Volume.136) (Chapter 69 Gor).

⁶⁰ Kiatchaloem Rakngam, "Legal Problem of the Determination of offenses concerning Computer Access According to Computer Crimes Act", *Journal of MCU Nakhondhat*, vol. 7, no. 9 (2020): 193–204. ThaiJo, via ThaiJo, <http://www.thaijo.org>.

⁶¹ Thanontus Suthiyantipakdi, "Computer Crime: a case study of the Prevention of Unauthorised Access to the computer systems", (Research Proposal Dissertation, Mahidol University, 2016), 15-19. Mahidol University, via Mahidol University, https://graduate.mahidol.ac.th/engine/current-students/detail/abstract_view.php?id=5636107&fac=25&prg=2508M&gp=04.

⁶² Government Gazette, Thailand Cybersecurity Act, (2019). (Volume.136) (Chapter 69 Gor) Section 3 "Critical Information Infrastructure" shall mean the computer or computer system that the Government Agency or private organization uses in their operations which relate to maintaining national security, public security, national economic security, or infrastructures in the public interest.

legal measures to address emergency cyber threats.⁶³ Moreover, CII units are actively involved with the significant national security agenda and classified information, including but not limited to sensitive data. Therefore, the CSA enforced the provision of explicit measures, whether the cybersecurity policy, the particular authority units, or specific measures such as notification law and data privacy impact assessment to handle and encounter cyber threats.⁶⁴ The CSA's primary responsibility is to support the central operation in dealing with cyber threats, mainly focusing on personal data breach incidents, whether they are frequent or critical substantial dangers to public infrastructures. The enforcement of the CSA framework among Thailand's governmental sectors illustrates its cognizance and conclusive measures in addressing cybercrime. Most of the provisions of CSA involve the administration because most of the CII units are operative in the public sector. The general description demonstrates that the CSA has a prominent role in arranging and handling the CII against cyber threats, whether at normal or serious levels.

The administrative authority was transferred to the Ministry of Digital Economy and Society (MDES) for supervision and compliance with the CSA. The critical unit within CSA is comprised of the National Cyber Security Committee (NCSC), the National Cyber Security Agency (NCSA)⁶⁵," and the specialized unit "Thailand

⁶³ Thailand National Cyber Academy, The summarisation operation report 2021-2022 by Thailand National Cyber Academy.

⁶⁴ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor), Remarks: "The reason for the enactment of this Act is that nowadays the provision of services or application of the computer networks, the internet, telecommunication networks, or general satellite services are currently under the risk of Cyber Threats which may threaten national security and public order in the country. In order to be able to simultaneously prevent or cope with Cyber Threats, it is deemed appropriate to determine the characteristics of the mission or services that are fundamental as critical information infrastructure, for both the government agency and private organization."

⁶⁵ Annual Report 2023 by the Thailand Personal Data Protection Committee (PDPC), Thailand Personal Data Protection Committee (PDPC) official website. https://www.pdpc.or.th/pdpc-book/annual-report-2566/?fbclid=IwY2xjawInxNdleHRuA2FlbQIxMAABHfYUXWTB2H3aAOGZqgpyRnaDymSlkMH2cE3F21Xv7OopME_SZv4YgxbgFw_aem_DuxdkwomzBcU4SILGmNvDQ (accessed 15 April 2024)

National CERT" to oversee, analyse, decide, and assess cyber threats affecting the Government Agencies sectors. In 2020-2021, NCSC, NCSA, and Thailand Computer Emergency Response Team (Thai CERT)⁶⁶ began operating under the National Cybersecurity 2022-2027⁶⁷ the framework was created after Thailand's government was notified of the outline of compliance responsibilities under Section 43 CSA.⁶⁸ The NCSC policy and operation scheme illustrates that NCSA functions as a public organization that implements policies and measures to create guidelines for maintaining cybersecurity in government agencies and private sectors. It also establishes a response team to address cyber threats. Thai CERT operated as the first responders to identify, investigate, and assess cyber threats, collaborating with Thailand's CCIB to hunt down and prosecute the perpetrators.

The focal principles under Thailand's CSA allude to the purview of law implementation under government agencies and may address the PDPA principles that might cause overlapping and loopholes in matters of government agencies. Thus, when the cyber threat and personal data breach happened, the duties to provide the appropriate cybersecurity system, Data Privacy Impact Assessment (DPIA), and data breach notification law were explicitly mentioned in CSA sections 54 and 56.⁶⁹ Moreover, with the declaration of subordinate legislation as "Notification by NCSC: the appropriate standard of cybersecurity for the information or internal cyber system 2023", this

⁶⁶ The summarisation operation report 2021-2022 by Thailand National Cyber Academy.

⁶⁷ Thailand's Ministry of Digital Economy and Society. (MDES) Government Gazette, The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update March 2024, (2020). <<https://www.mdes.go.th/law>> (accessed 15 May 2024). "Notification by NCSC : the main policy and the strategic plan of Naition Cybersecurity 2021-2027" (Volume 139) (Special Chapter 288 Ngor), date enacted: 9 December 2021.

⁶⁸ Government Gazette, Thailand Cybersecurity Act 2019. (Volume.136) (Chapter 69 Gor), Section 43.

⁶⁹ Ibid. Section 54, and Section 57. According to CSA, the definition of "notification" use the term as "report" to the authority (Thai CERT) when the cyberthreats occurred.

secondary regulation follows CSA in providing the definition of the CIA principle.⁷⁰ This secondary regulation could be a confrontation with CSA section 60 regarding the issues of cyber threat management.⁷¹

The principle emphasized the importance of conducting a Data Privacy Impact Assessment (DPIA) to prevent personal data breaches.⁷² This assessment involves testing the internal security system, categorizing types of personal data, ensuring confidentiality and following CIA principles. It also includes assessing cyber threats and implementing recovery and urgent action measures for breaches affecting national security. DPIA evaluates the potential actions for individuals affected by personal data breaches. The PDPA principles will govern this provisional compensation, which will be expanded in the next section. Significantly, the actual measures after doing DPIA as provided in “Notification by NCSC: the distinctive of cyber threat prevention measures, encounter, evaluation, suppression and restrain the cyber threat in each level (2021).” These principles under CSA are specifically differentiated from PDPA in that

⁷⁰ The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand’s Ministry of Digital Economy and Society. (MDES) Last update: March 2024. “Notification by NCSC: the appropriate standard of cybersecurity for the information or internal cyber system 2023” (Volume 141)(Special Chapter 18 Ngor) Date enacted: 18 January 2024. Confidentiality shall mean safeguarding limited access or disclosure of personal data for external persons and organisations, including restricted data trafficking., Integrity shall mean safeguarding data integrity., Availability means any operation or instructions for an individual or organisation to access and use the systems and data at any time and effectively. Notification number 4: The organisation under CSA shall be responsible for determining the security category concerning the importance of CIA principles. Notification number 5: In terms of doing a Data Privacy Impact Assessment, the determination shall be into three levels: Low, Medium, and High on the importance of confidentiality in each piece of information or data

⁷¹ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor), Section 60

⁷² Ibid. Sections 57,58, and 60. Regarding the DPIA principle, it is limited to CII units and government agencies in which the scope is explicitly in CSA only. Large enterprises, such as the private sector, may not even be subject to CSA, but these private sectors may select doing the DPIA as the best practice to follow the appropriate security measures.

they are used to encounter and respond when “cyber threats”, including personal data breaches, occur in CII units.⁷³

The principles defined in Thailand's CSA and related legislations largely align with regulations, focusing on maintaining security standards, preparing for cyber threats such as personal data breaches, and categorizing and organizing internal information systems and databases based on DPIA principles. Implementing legal measures to prevent and address personal data breaches, a typical cyber threat, and immediately notifying the NCSC when such threats arise is a way of adapting and contextualizing the original PDPA principles within the framework of Government Agencies. Since PDPA structures may have specific provisions exempting government sectors from enforcement, the CSA serves as the best solution to guide and clarify the interpretation and implementation of the law. The principles include the Sanction and Liability section 70-72 of CSA.⁷⁴ Another category of liability is non-compliance. This category is essential to address the circumstances of cyber threats and the specific execution of actions against such threats, particularly in critical or urgent crisis situations as

⁷³ Government Gazette, the subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update: March 2024. Notification by NCSC: the distinctiveness of cyber threat prevention measures, encounter, evaluation, suppression, and restraint of cyber threats at each level (Volume 138) (Special Chapter 303 Ngor) Date Enacted: 11 December 2021. This regulation extended the elaborations of the approaching measures through the compliance of DPIA, which is regulated as Pre-Incident measures. Moreover, CSA carried out the “Detecting measure” combined with containment eradication and recovery measures to arrange the personal data breach incident overall. Lastly, Post-Incident measures shall be applied to enhance the victim's security system and the authorities tackling the cybercriminal for the law execution under CSA, CCA, and Penal code, depending on each incident.

⁷⁴ Government Gazette, Thailand Cybersecurity Act 2019. (Volume.136) (Chapter 69 Gor), Section 70 to 72

Section 70 The officers under this Act shall not disclose or send computer data, computer traffic data, other data related to the computer system, or data of the users obtained from this Act to any person. Any officer violating shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both. Paragraph one shall not apply to act for the benefit of litigation against an offender under this Act or an offender under other laws or for the benefit of the litigation against the officer related to the exercising of unlawful authority.

Section 71: Any officer under this Act negligently causing other persons to know computer data, computer traffic data, data of the users, or other data related to the computer system obtained from this Act, shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.

stipulated in sections 73-76 of Thailand's CSA. The notion that encompassed the perpetrators under the CSA about "Juristic person" has also been integrated into Thailand's PDPA, utilizing the legal concept of "Cooperate Veil" to address the potential liability gap for organizations in relation to offences. The sanction of the CSA is outlined in Section 77.⁷⁵

The criminal liability sanction focuses on dealing with the offender through their duties, including ensuring the officer under CSA compliance with the "CIA Principle." Violations of responsibilities will be subject to criminal penalties and fines. The specified offences under CSA aim to clarify and prevent confusion or ambiguity in the Penal Code Criminal Offences and CCA criminal offences. However, the CSA plays a prominent role in encounter, suppression, and recovery, specifically regarding "cyberthreats" issues. Therefore, it should address explicit clarification in terms of the implementation between CSA and CCA as another legislation applied to the subject of the ICT system, and the liabilities are similar elements regarding the computer-related and cyberthreat intersection characteristics.

This is the central explanation for implementing special sanctions for unauthorized or harmful conduct inside the CSA framework. Significantly, the CSA framework plays a crucial role in 2023 regarding the encounter with cyberthreats. As

⁷⁵ Ibid. Sections 73-77. It is highlighted that the Non-compliance sanction regarding the CSA framework focused on the authority not doing the "cyber threat incidents report" under sections 57-58 but the "Notifications duty" conducted as optional as mentioned in subordinate legislation.

Section 73 Any Organization of Critical Information Infrastructure not reporting a Cyber Threat incident in accordance with section 57 without reasonable cause shall be subject to a fine not exceeding Baht two hundred thousand.

Section 74 Any person not complying with the summoning letter of the Competent Officials, or not sending information to the Competent Official in accordance with section 62 (1) or (2) without a reasonable cause, as the case may be, shall be subject to a fine not exceeding Baht one hundred thousand.

Section 77 In case the person committing an offense under this Act is a juristic person, if such offense is a result of the order or the act of a director or a manager or any person responsible for the operation of such juristic person or in case such person has the duty to order or act and omit to order or act, causing the juristic person to commit an offense, such person shall be liable for the penalties prescribed for such offense

part of the operation of the Thai CERT unit, the officers are under CSA, CCIB, and MDES's immediate response. The exposure was leakage of sensitive data in the crisis, as potential elderly populations' personal data breach instances in February 2024⁷⁶, and the Ministry of Health's unauthorized access intrusion in March 2024 is the urgent cyberthreats that harm the significant CII units as the healthcare and the elderly information infrastructures.⁷⁷ In short, the CSA is upcoming as the prominent legislation to suppress the cyberthreats and fill the lacuna regarding the encounter, management, and actual operations in which CCA and the Penal Code did not regulate these measures. Meanwhile, the primary accountability legislation regarding compliance duty, specifically under the subject of personal data, will be provided with elaboration in the next part of PDPA 2019.

3.6 PERSONAL DATA PROTECTION ACT 2019 (PDPA)

As mentioned above, PDPA recognizes the significance of personal data by dividing it into two categories: personal data⁷⁸ and sensitive data.⁷⁹ The data controller must apply specific measures to collect, process, and disclose legitimately. The primary entities under PDPA are:

⁷⁶ *Thailand Consumer Council*, "MDES Strengthen Department of Older Persons into Notified and Clarification to the Elderly Injured Person Regarding the Recorded of 20 Million Personal Data got Hacked. ", *Thailand Consumer council*, 2024, February 9. https://www.tcc.or.th/09022567_elder-information-leak_news/ (Accessed 25 March 2024)

⁷⁷ *Matichon Online*, "Ministry of Health Clarified that the Hacker Posted the Sell the Patient's Data is Fake. The Ministry Confirmed that the Personal Data was Not Leaked from the Ministry of Health Systems," *Matichon Online*, 2024, March 19. https://www.matichon.co.th/local/quality-life/news_4480163 (Accessed 19 March 2024)

⁷⁸ Government Gazette, Thailand Personal Data Protection Act 2019. section 6 Personal Data” means any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular

⁷⁹ Thailand Personal Data Protection Act 2019. (Volume.136) (Chapter 69 Gor), Section 26 Any collection of Personal Data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Committee, is prohibited, without the explicit consent from the data subject, except where: it is to prevent or suppress a danger to life, body or health of the Person, w h e r e the data subject is incapable of giving consent by whatever reason

1. Data Subject⁸⁰
2. Data Controller⁸¹
3. Data Processors⁸²

These three vertices distinguish them from the other amendments, such as the Penal Code, CCC, CCA, and especially CSA. Through the adaptation function under the legal transplanted methodology, the PDPA framework applied the rudimentary principles from EUGDPR as follows:

1. The Data Controller shall collect, gather, process and disclose personal data under the legitimate interests and purposes.⁸³ Moreover, when processing all the personal data from the data subject, the data controller requires the validity of the legal basis, such as consent, contract, legitimate interest, and legal obligations.⁸⁴ It could be declared that PDPA reflects the lawfulness, transparency, purpose limitations, and data minimization of the EUGDPR⁸⁵ regarding the relationship between the Data Subject and Data Controller in PDPA.
2. The accuracy purpose limitation and data minimization principles PDPA has also been adapted from EUGDPR and enshrined in the duties of data controller into collection, process, and usage (disclosure) under a lawful basis.⁸⁶ Moreover, the primary rudimentary principle of information security

⁸⁰ Ibid. Chapter 3 Sections 30-34

⁸¹ Ibid. Section 6 “Data Controller” means a person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data”

⁸² Ibid. Section 6 “Data Processor” means a person or a juristic person who operates in relation to the collection, use, or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such Person or juristic person is not the Data Controller

⁸³ Ibid. Section 19

⁸⁴ Ibid. Sections 24 and 26

⁸⁵ Narong Jaihar, et al., *General Data Protection Regulation (Thailand’s description version)*, (Thailand: T.press Ltd., 4th ed.,2022).

⁸⁶ Government Gazette, Thailand Personal Data Protection Act 2019. (Volume.136) (Chapter 69 Gor), Sections 27 to 29.

as confidentiality, availability, and integrity (CIA) directly involved with personal data breach incidents obliged the data controller to comply with the provisions of PDPA, such as providing the appropriate security system and notifying when a personal data breach occurs.⁸⁷ This reflection of crucial principles of EUGDPR demonstrates the data controller's compliance duty in the PDPA structure. Furthermore, the compliance duty related to the non-compliance sanctions ensures that personal data is sufficiently protected by the Data Controller's responsibility and the authority's (PDPC) subordinate regulations.

3. Finally, the critical principle of accountability in the PDPA is inspired by the EUGDPR's appointment of the supervision authority as PDPC.⁸⁸ Also, there is a requirement for special personnel to be Data Protection Officers (DPO).⁸⁹ This principle upholds the standard of compliance in both internal organizations and external authorities. DPO's internal guidance, audit, and examination supervision by PDPC shall include and guarantee that personal data protection principles are effectively enforced. Furthermore, the PDPC authority has extra power to investigate and to impose the sanction under the proceeding in relation to the infringement of PDPA.⁹⁰

In short, the structure of PDPA demonstrates important and specific subjects, principles, and duties regarding personal data protection. However, some principles of PDPA, such as providing the appropriate safeguard system, are similar to those of the

⁸⁷ Ibid. Sections 37 (1) and (4)

⁸⁸ Ibid. Section 43

⁸⁹ Ibid. Section 41

⁹⁰ Ibid. Chapter 5 Complaint: Section 71

CSA framework.⁹¹ The purpose of the law remains distinct, because PDPA provides the inclusive personal data protection principle and the responsibility organization. Both the private (Data Controller) and the government (Authority) also have significant personal data owner (Data Subject) relations. The next part will discuss the rudimentary principles of PDPA and elaborate on the rights of the data subject.

3.6.1 Data Subject Rights

The rights of individuals who are the subjects of data processing are provided in PDPA Chapter 3 of the PDPA 2019⁹² They are as follows;

1. Right to withdraw consent (Section 30, paragraph 1)
2. Right to access, obtain, and copy personal data (Section 30, paragraph 1)
3. Right to receive personal data in machine-readable formats and request the data controller to send the same to another data controller (Section 31, paragraph 1)
4. Right to object to the collection, usage and disclosure of personal data in the circumstances as set out in the PDPA (Section 32, paragraph 1)
5. Right to request for deletion and anonymisation of the personal data in the circumstances set out in the PDPA (right to be forgotten) (Section 33, paragraph 1)

⁹¹ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor), From CSA framework provides special measures to arrange the cyber threat situations when they occur in the CII units.

⁹² Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Sections30-34

6. Right to request a suspension of use of the personal data in the circumstances set out in the PDPA (Section 34, paragraph 1)
7. Right to maintain the accuracy of processing of personal data (Section 35)
8. Right to file the dispute under the complaint principle to the authority (PDPC) (chapter 5 of PDPA)⁹³

These regulations emphasise that in the event of personal data breach incidents, the right to complain is necessary for an investigation by authority. Moreover, maintaining accurate records and processing personal data relates to the Data Controller's obligations to uphold the information security principles. Furthermore, the complaint has a crucial role in administrative liability, expanding to other liabilities under the sanctions part and shall be cross-checked by the judiciary. It is emphasised that the Data Subject requires an essential awareness of using the “complaint” rights and other rudimentary rights in the PDPA.⁹⁴

3.6.2 Data Controller Compliance

Primarily, data controllers and data processors who usually coordinate personal data activities, whether collecting, gathering, processing, usage and disclosing under legitimate interests and basis and righteous purposes, have to comply with duties under Thailand's PDPA section 37 (1) and 40.⁹⁵ The principles were implemented in the "Notification of PDPC Thailand's 2023: The fundamental standard of the security system of a data controller who received an exemption under Thailand's PDPA."

⁹³ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor).

⁹⁴ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya", Bangkok, 14 May 2024, The representative addressed the issues of data subjects, who usually mislead into complaints to PDPC by misunderstanding and misinterpreting the principles. Mostly, the Data Subject require compensation from the Data Controller, which this agenda requires to file to the Civil Court.

⁹⁵ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor).

Furthermore, the CIA principle was specified and incorporated into Thailand's Cybersecurity Act 2019 during the simultaneous development of the laws.

The relationship between CSA and PDPA can be highlighted through the PDPA principle, which should be considered the distinct overarching notion pertinent to the passage. The CSA of Thailand supervises compliance with Information Security standards, providing superior interpretations and implementations for government agencies and Cyber Threats compared to the PDPA. Nevertheless, the subjective nature and regulatory compliance under Thailand's PDPA framework does not align with the CSA principles due to the clear division of responsibilities and authorities outlined in the subordinate legislation, which includes supervision and accountability entities such as NCSC, NCRC, NSCSA, and Thai Cert.⁹⁶ The PDPA provides for a central PDPC section that is responsible for managing and coordinating responses to personal data breach incidents.⁹⁷

Secondly, another convergence between the PDPA and CSA is the duty to notify when a personal data breach occurs. PDPA's data controller shall inform PDPC⁹⁸ of the incident under "Notification of PDPC Thailand's 2022: The principle of data breach notification". Connectivity with the sanction under Section 90⁹⁹ demonstrates that the

⁹⁶ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor),

⁹⁷ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), in. From the complaint function under the PDPC Thailand investigation, the authority could specify the administrative sanction only. For the other liabilities, the Data Subject or injured person shall file the lawsuit directly with the court under this law and fundamental legislation as CCC and Penal Code.

⁹⁸ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Section 37 (4) Section 37 The Data Controller shall have the following duties: (4) notify the Office of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of the Persons. Suppose the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Persons. In that case, the Data Controller shall also notify the Personal Data breach and the remedial measures to the data subject without delay. The notification and the exemption to the notification shall be made in accordance with the rules and procedures set forth by the Committee

⁹⁹ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Section 90 The extension of the description shall follow Notification of PDPC Thailand (subordinate legislation) as the terms of the direction to specify the Administrative sanction order following section 90 of Thailand's PDPA 2019.

dispute resolution process in the PDPA framework by PDPC Thailand is more comprehensive than that by the OCPB (Office of the Consumer Protection Board)¹⁰⁰ Structure. The Notifications Law might resemble to the CSA framework, as the duties to notify the authorities, based on the PDPA framework, focus on the notice of the Data Subject as primary. Hitherto, the CSA highlights the encounter of cyber threats. Therefore, the issues of notification laws might cause the misunderstanding of overlapping conflict if the Data Controller cannot precisely exercise regarding this compliance provision.¹⁰¹

Significantly, the definition of a personal data breach. is finally stipulated in Thailand's legal framework, as not referred to in the other enactments. In the PDPA, section 37 (4) goes further on the Notification of the PDPC Thailand's 2022. The idea of data breach notification, as outlined in the PDPC Thailand's 2023 regulations, establishes the rudimentary criteria for the security system of data controllers exempted under Thailand's PDPA. Continuously, The definition of a personal data breach under subordinate legislation suggests that the "CIA principle violation" term encompasses the original illegal activity related to ICT systems crimes regarding unauthorised access. The concept of a personal data breach was also found in the NCSA Annual Report 2022,¹⁰² where the terms closely correspond to those in the PDPA's subordinate legislation. The concept of a personal data breach centres on information theft and any

¹⁰⁰ Thawat Buapitak Vice presiding Judge of Udon Thani Provincial Court, "The Principle of Piercing the Corporate Veil with consumer protection", *Official Court of Justice articles COJ library*, via Court of Justice library, <https://library.coj.go.th/pdf-view.html?fid=51341&table=files_biblio>. (Accessed 15 April 2024).

¹⁰¹ Annual Report 2023 by the Thailand Personal Data Protection Committee (PDPC). The notification issue in PDPA is the strict compliance duty of PDPC. Meanwhile, in the CSA framework, the strict duty is to do a "high and emergency cyber threat" notification "report" to NCSA and Thai CERT for encountering the threats, and the Notification law is optional.

¹⁰² Annual Report 2022 by Thailand National Cyber Academy (TNCA). The significant connectivity between PDPA and CSA found that PDPA should investigate compliance duty and prevention measures. Meanwhile, the CSA framework shall launch the detection, suppression, execution, and recovery measures in the event of a Personal Data Breach.

actions involving illegal access. According to the CSA principle, precisely the secondary principle of notifications law, government agencies must notify about personal data breaches, consider cyber threats, and take appropriate measures outlined in the CSA principle. Eventually, the definition of personal data breach outlined in the subordinate legislation may pertain to the legal status of the issue, suggesting that unlawful acts should generally be recognised explicitly in the PDPA 2019. Nonetheless, the PDPA mandates that these unlawful actions compel the "Data Controller/processors" to adhere to requirements, including but not limited to implementing adequate security measures, disclosing personal data breaches, and incurring repercussions for non-compliance. Individuals affected by a data breach could report directly to the PDPC Thailand or file a lawsuit based on PDPA principles and potential sanctions.

Finally, appointing a Data Protection Officer (DPO) is regulated in Section 41 of PDPA.¹⁰³ The Data Controller has a duty to have these personnel in the organisation. The main role of the DPO in Section 42 of PDPA is to check and balance the internal processing of personal data and control the Data Controller to strictly comply with Section 26 (sensitive data issues).¹⁰⁴ Regarding personal data breaches, the DPO shall notify the PDPC within 72 hours post the data controller gets to know the incident occurring so that immediate response and coordination can be obtained with the authorities. However, the exemption of PDPA enforcement indicates that certain sectors are excluded from specific activities through subordinate laws like "the Notification of PDPC Thailand 2022," which exempts small and medium-sized firms.¹⁰⁵ The

¹⁰³ Government Gazette, Thailand Personal Data Protection Act 2019 (Volume.136) (Chapter 69 Gor), . Section 41

¹⁰⁴ Ibid. Section 42 (1) – (3)

¹⁰⁵ Government Gazette, The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society.

anticipated negative impact is predicted to be minimal, and there may be an inadequate budget for cybersecurity investment. Some government activities or sectors have profited from Section 4 of the PDPA, such as the company under the credit card financial regulation.¹⁰⁶

The exemption principle may result in insufficient awareness of the Data Controller's extensive compliance obligations. The Data Protection Officer (DPO) serves as the public authority representative under the Personal Data Protection Act (PDPA) and plays a crucial role in overseeing the organisation's internal operations and coordinating with the Personal Data Protection Commission (PDPC). Additionally, Data Protection Officers are mostly designated in major organisations, such as CII units. Simultaneously, SMEs benefiting from the exemption principle may neglect to maintain the internal security principles of confidentiality, integrity, and availability (CIA). The absence of communication during a personal data breach may significantly exacerbate the client's data vulnerability. This matter necessitates careful consideration, and authority must diligently address the task of thoroughly disseminating an understanding of the Personal Data Protection principle inside the organisation. From the compliance duty description, the next part will describe the inclusion of PDPA sanctions.

(MDES) Last update: March 2024. Notification by PDPC Thailand: the data breach notification procedures. (Volume 139) (Special Chapter 292 Ngor), Date Enacted: 15 December 2022. *Notification number 3: Personal Data Breach shall mean the violations of the security system which contributed to the losses, accesses, usage, adjustment, editing or disclosures of personal data in terms of unauthorised or illegitimately. These actions include being committed by intent or negligence, unauthorised, unlawfully engaging in computer-related crimes, launching cyber threats, or any errors and accidental incidents. Notification number 4: the confidentiality breach shall mean the unlawful Illegal access or disclosure of personal data, including errors and accidental incidents., The integrity breach shall mean the unlawful adjustment or editing of personal data into incorrect or incomplete by unauthorised access or any errors and accidental incidents. , The Availability breach shall mean unlawful restrain accessible for regular personal data usage or any disruption or destruction of personal data, which includes any action that affects the regular usage of personal data*

¹⁰⁶ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Section 4

3.6.3 Civil Liability

Civil liability in PDPA could be imposed under Sections 77 and 78.¹⁰⁷ Eventually, the victim must file a lawsuit in court. The PDPA principles must be established through relevant procedures such as the Intellectual Property Court. Therefore, the side will submit the case to the civil court for civil liability. Sections 77 and 78 are invoked under the Strict Liability principle regarding internal proceedings in the Notifications Law. Consequently, the exemption for the Data Controller seems to restrict the breadth of the "Act of God". It imposes an additional expense to alleviate the effects of personal data breaches experienced by Data Subjects.¹⁰⁸ Strict accountability for the Data Controller is justified by the crucial duty to ensure the security and protection of personal data. The PDPA enforces regulations in both private and public sectors.¹⁰⁹

The concept of "Immaterial damage" poses challenges for data subjects in proving harm, particularly in personal data breaches involving cybercrimes that may be difficult for individuals to explain and demonstrate in court. In case No.610/2539 (1996), the court examined the legal remedies under section 446 of CCC. The defendant was found to erect a structure incorrectly through non-compliance of safety procedures, resulting in construction material falling onto a person and causing injury. The plaintiff demanded psychological therapy. Hitherto, the court concluded that the Plaintiff might seek compensation, including but not limited to actual damages, from the defendant due to the defendant's negligence. The extensive personal data breach leads to widespread cybercrime, affecting many individuals claiming intangible compensation. This would

¹⁰⁷ Ibid.

¹⁰⁸ Government Gazette, Thailand civil and commercial code.(Volume 141) (Chapter 58 Gor) (Revised 2024).” Section 8. "Force Majeure" denotes any event the happening or pernicious result of which could not be prevented even though a person against whom it happened or threatened to happen were to take such appropriate care as might be expected from him in his situation and in such condition.”

¹⁰⁹ Theerachit, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act and EU's General Data Protection Regulation (EUGDPR)".,52-55.

require the victim to explain themselves. The PDPA provision enforces the punitive concept instead of addressing the potential damages within three years after the personal data breach occurred.¹¹⁰

The civil liability under PDPA characteristics are similar to those of The Consumer Protection Act and Consumer Protection Procedure Act, particularly in applying Strict Liability and Punitive principles as specified in Section 42 of the Consumer Protection Procedure Act. Although the PDPA provision has been fully enforced for the first five years, the regulations regarding personal data breaches are still under review as of June 2023. Compensation for personal data breaches may follow consumer protection principles. Case number. 4189/2563 (2020) originated from an internal hearing where the consumer committee resolved a disagreement between a resort and 62 clients who had booked services at the resort. The clients could not access the defendant's services, and their attempt to return the booking cost was invalidated by the service provider. The rudimentary issue concerns the defendant exploiting or attempting to deceive the consumer into using and buying their services. According to Section 29 of the Consumer Protection Procedure Act, the burden of proving lies with the defendant's service provider if the defendant cannot substantiate the exemption or any claim that they are not enticing clients to utilize their service. The court has ruled that the defendant has to repay the clients based on the actual financial transactions. The defendant will be required to pay the plaintiff extra punitive damages, without interest, due to their deceptive actions in enticing clients to utilize their services at the resort.¹¹¹

In summary, Thailand's civil liability due to the data breach consists of two primary stages.

¹¹⁰ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor),

¹¹¹ Ibid.

1. The Personal Data Breach Notifications Law mandates that the Data Controller and PDPC authority address and settle the dispute before the dispute is filed to initiate judicial proceedings. This provision will continue throughout the investigation since several cases have commenced filing complaints against data controllers who have encountered personal data breaches. Victims of cybercrime are anticipated to obtain prompt interim assistance during this provisional phase.

2. The damages specified of PDPA in section 77 are more limited than those specified in the CCC. They apply exclusively to the responsibility of Data Controllers and Data Processors in safeguarding Data Subject information. Section 78 of the PDPA provides punitive measures, including expected payment for long-term damage resulting from a personal data breach. Meanwhile, the immaterial damages issues will implemented under CCC's principles. Enhancing claims for immaterial damages by the victim may not immediately apply within the PDPA Civil Liability structure. However, this type of compensation may also apply in a different area of punishment, specifically criminal punishment for personal data breaches under PDPA. An individual harmed may seek non-monetary compensation under Section 44/1 of CRPC¹¹², which is connected to the general tort principle in CCC. Another possible approach for enhancing the legal process for numerous individuals affected by personal data breaches in Thailand is implementing the "Class Action" principle in the CPC.¹¹³

¹¹² Government Gazette, Thailand's Criminal Procedure Code.(Volume 134) (Chapter 69 Gor) (Revised 2017). Section 44/1-44/3

¹¹³ Government Gazette, Thailand civil procedure code.(Volume 136) (Chapter 34 Gor) (Revised 2019), Section 222/1-222/49

3.6.4 Criminal Liability

The second sanction category under PDPA is the sanctioning of criminal liability, as the terms of the “Penalty” are enshrined in section 79, chapter eight of PDPA. Moreover, section 80 expands the scope of the criminal offence by interpreting "Data Controller" as "Any person" and includes an exemption from liability based on the criteria outlined in section 4 of PDPA. The PDPA primarily focuses on illegal actions that could harm the data subject or personal data owner, specifically the unauthorized disclosure of personal data. Both individuals and legal persons, such as companies or organizations, can be held liable under Section 81 of the Act.¹¹⁴

The "Corporate Veil"¹¹⁵ principle addresses situations where a company is an offender and ensures that legal loopholes related to non-natural persons are covered. The judicial branch can reasonably use the principle of "Proportionality" when specifying punishment in section 81. The "Ultra Vires" principle will not limit the decision even if it exceeds the prescribed liability framework. The Corporate Veil principle is expected to be applied to impose civil liability sanctions to ensure that the injured party receives compensation. Furthermore, the principle may be implicitly applied in administrative procedures and decisions to hold the offender accountable, ensuring that legal organizations can also be held liable under PDPA. Sections 79 to 81 outline the liabilities associated with the role of a Data Controller, distinct from the roles defined in CSA and CCA frameworks. The CCA framework addresses computer-related crimes as a precursor to "Illicit disclosure of personal data." The criminal liabilities provisions under these three Acts did not overlap due to PDPA criminal liabilities implemented in the specific components regarding the illegal disclosure of

¹¹⁴ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Section 79-81

¹¹⁵ Thawat, "The Principle of Piercing the Corporate Viel with consumer protection".

personal data. Regarding law implementation, the 9-Near crisis has undergone massive investigations and the culprit will be held accountable under section 79 of PDPA, as stated by the minister. If 9-Near happens to be an officer within the CSA criminal offences, he is liable for criminal liability under the CSA. Illegal publication of personal data by a Data Controller with unlawful intent will result in liability under the PDPA, effective after 1 June 2022 in the "Post-enforcement" period.¹¹⁶

3.6.5 Administrative Liability

Thirdly, the administrative liability under the jurisdiction of the PDPA is explicitly mentioned in section 83 concerning Personal Data Breach incidents, the Data Controller and Data Processors failed to adhere to essential requirements, including the requisite security measures outlined in section 37(1), compliance by Data Processors as stipulated in section 40(2), and the Data Breach Notification Law specified in section 37(4) of the PDPA. Moreover, the actual procedure under administrative sanction shall be conducted with the additional subordinate legislation as “Notification by PDPC Thailand: The main principle into specify administrative order sanction under expert committee (2022)”.¹¹⁷

Sanctions for non-compliance in this category may be enforced through administrative liability. Conversely, optional attempt to infer from the EUGDPR as the majority of data controllers and processors are large corporations or reputable companies in the private sector. The public sector is focused on large-scale activities and essential functions, such as those carried out by the Ministry of Health. However, the implementation of this sanction, the category belongs to the authority of PDPC to

¹¹⁶ *BBC Thai*, "9near : จับกุม จำคุก โท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว" ("9-Near surrender himself the hacker who claimed that earned 55 million record of Thailand's population data"), *BBC Thai*, 2023, March 31. <https://www.bbc.com/thai/articles/cq5z3w5lwdxo> (accessed 15 May 2024)

¹¹⁷ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Sections 83,86, and 90.

provide the statements. Hence, the effectiveness of the Non-compliance sanction implementation will belong to the “Privacy Awareness” among data subjects who earned the complaint rights in Chapter 5 of PDPA 2019. This category of the PDPA framework focuses on the complaint and administrative non-compliance status related to Administrative Action and Administrative Order by the authority (PDPC), derived from Thailand's administrative legal framework.

CSA adheres to the same principle with respect to the notification regarding the appeal process and the ability to file a direct lawsuit in the Administrative Court, as stated in section 69.¹¹⁸ It is advisable to thoroughly investigate and analyse the administrative dimensions of the PDPA and CSA framework to assess the efficacy of law interpretation and implementation due to the discretionary nature of administrative proceedings and the unique procedures studied in this legislation.

3.6.6 The milestone incident: JIB Computer

Thailand's PDPC effectiveness was taken in a case known as the "JIB personal data breach" in March 2024. JIB is a famous corporation that sells ICT products and offers maintenance, modifications, and additional ICT accessories. In March 2024, some victim began to suspect that some of JIB's clients were contacted by the Call-Centre Gang, who revealed precise information about their purchasing history from JIB, including dates, times, product serial numbers, and prices. Thus, JIB's client opted to bring up and deal with this issue through a complaint to the PDPC Thailand. The PDPC

¹¹⁸ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor),” Section 69: A person receiving an order related to coping with a Cyber Threat may only appeal such order for Cyber Threats at a non-critical level.”

Eagle Eye¹¹⁹ Unit and Thailand's CCIB were notified in the JIB report after the incidents occurred.¹²⁰

Based on testimony and declaration from JIB computer company, the subsequent investigation was conducted, and it was discovered that:

1. The personal data breach incident is confirmed as the complaint.
2. JIB accused that the personal data breach incident might have happened by an ex-employee of JIB who illegally sold personal data to cybercriminals
3. JIB has informed PDPC Thailand under the “Data Breach Notification Law”, but PDPC¹²¹ observed that JIB didn’t comply with section 37(1) appropriately and did not appoint a “Data Protection Officer (DPO)”. Also, JIB did not take any measures to provide a tentative remedy to the data subject, which PDPC has ordered JIB to review the internal security system measures and additional rectify the security system.
4. Currently, JIB provides tentative treatment remedies to the data subject as the remedy and compensation under the supervision of the Expert Committee.

In August 2024, PDPC issued a statement relating to the investigation of the JIB personal data breach incident as follows:

1. JIB neglected to designate a Data Protection Officer in the office despite the compliance requirement since the large organization was handling over 100,000 personal data units. The DPO appointment is mandatory as a

¹¹⁹ Personal Data Protection Committee, "PDPC Prompted the Special Unit Called Eagle Eye to Monitor the Personal Data Breach Situations.", <<https://www.pdpc.or.th/2640/>>. (Accessed 15 April 2024)

¹²⁰ Personal Data Protection Committee Thailand, "The Tentative Declaration in the “JIB” Personal Data Breach Case by Thailand’s PDPC”, the Declaration of the "JIB" Personal Data Breach Facts., <https://www.facebook.com/story.php/?story_fbid=433047432569353&id=100075923001714&paipv=00&eav=AfbXcfn5685uYNgrNa_yXa3ziKLG55YxAlnKaS52ylNSlkv8UXs4QxgqEfFO6M8GWzM&_rdr>. (Accessed 15 August 2024)

¹²¹ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor),” Section 74”

complaint under the PDPA. JIB received a penalty of 1 million Baht for this offence.

2. JIB did not provide the appropriate security system, as the Data Controller failed to comply as provided the adequate security system under Information Security principles. Thus, JIB was fined 3 million Baht.
3. JIB did not notify PDPC within 72 hours of the personal data breach incident, a non-compliance under Sections 83 and 37 (4). Therefore, JIB is liable for an administrative fine of 3 million Thai Baht (THB).¹²²

The total administrative fine is THB 7, a very high rate for punitive sanction for authority. Eventually, JIB Computers were penalized and were obliged to announce a declaration to the PDPA and perform following:

1. Enhancement of the Internal Security system inclusively;
2. Appointing expert personnel in the capacity of a DPO and the cybersecurity team,
3. Grooming and training the internal personnel,
4. Arrangement of the Compensation and Remedies to the client, who is the Data Subject and victim of the crime, and
5. Clarifying the policy direction so as not to contact clients directly.¹²³ This announcement remains under the supervision of the PDPC, which is now engaged in

¹²² PDPA Thailand, The First Decision From PDPC Thailand : An Administrative Fines in the Personal Data Breach Incident. <https://pdpathailand.com/pdpa-news/personal-data-protection-1st-fine-penalty/?srsltid=AfmBOoqndqP1hTaQmjRWccVe0zfk8jMPLnsmimvv-i7X6xnBgCgJGzf8> (Accessed 24 August 2024)

¹²³ JIB Computer Co, Ltd., The Official Announcement : The Maintenance Direction and Measures by JIB Computer Co, Ltd. (JIB Computer Official Facebook page, 2024). <https://www.komchadluek.net/news/social/584139> (Accessed 24 August 2024)

recovery efforts in accordance with government laws pertaining to cybersecurity matters.¹²⁴

The JIB incident exemplifies the substantial advancement in PDPA functions, highlighting the role of PDPC in actual examinations and the enforcement of penalties. It also emphasizes the implementation of recovery and maintenance measures for internal security aimed at upholding the principles of Information Security (CIA) and ensuring accountability in PDPA performance.¹²⁵ Meanwhile, the turning point of the CSA framework's success in the 9 Near operation is to handle the upcoming severe cyber threats immediately.¹²⁶ The effective implementation of the specific provisions of PDPA and CSA can demonstrate this. It is emphasized that these two laws shall continuously perform on standard and support to reduce the lacuna and legal issues in the other legislations, such as CCA, CCC, and Penal Code. Furthermore, it is determined that these two provisions (PDPA and CSA) are the primary challenges in the cyberlaw field in Thailand and shall act as the main characters linked with the rudimentary amendments to enhance Thailand's legal framework.

3.7 CONCLUSION

The current study showed that the legal transplanted phenomenon between 2000 and 2017 significantly impacted Thailand's legal framework, specifically in addressing the prevention, suppression, response, recovery, and treatment of personal data breach incidents under the leading role of the PDPA. This involves the collaboration between government agencies under the CSA and the enforcement of criminal liabilities outlined

¹²⁴ PDPA Thailand, The First Decision From PDPC Thailand : An Administrative Fines in the Personal Data Breach Incident.

¹²⁵ Ibid.

¹²⁶ *BBC Thai*, 9near : จับกุม จำคุก โท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว "9-Near surrender himself the hacker who claimed that earned 55 million record of Thailand's population data", *BBC Thai*, 2023, March 31. <https://www.bbc.com/thai/articles/cq5z3w5lwdxo> (accessed 15 May 2024)

as ICT Systems crime in Thailand's CCA. Thailand's Penal Code and Thailand's CCC provide the relevant provisions for individuals responsible for hands-on breach. Simultaneously, tort law principles provide additional remedies and compensation for specific and punitive damages under Thailand's PDPA.

The summarisation table 3.1 illustrates the role of the PDPA in guiding the specific arrangements and measures for government agencies concerning Cyber threats and personal data breach. Eventually, CCA, in its explanation of the second revision, has reinforced its role and the confrontation with the primary legislation, which are the PDPA and the CSA, in structuring the rudimentary criminal liability concerning ICT Systems-related offences and the escalating penalties directed at specific targets, particularly public infrastructure, as a primary strategy for addressing the actions of perpetrators. The primary legal framework is the Penal Code, which governs essential criminal liabilities. Simultaneously, Thailand's CCC extended the Tort Law principle to cover the additional remedy, whether from Data Controllers and Data Processors in the context of PDPA or the offenders in the context of cyber criminals, as the specific liabilities mentioned in the Penal Code and the CCA.

Based on this discussion, the research shall continue with the critique part of Thailand's legal framework assessment, the benchmarking analysis between Thailand's PDPA and the EUGDPR, and the future direction of personal data breach vide Artificial Intelligence in the next chapter.

CHAPTER FOUR

THE LEGISLATION BENCHMARK ANALYSIS AND THE FUTURE DIRECTIONS OF PERSONAL DATA BREACH LAW

4.1 INTRODUCTION

Hitherto, Table 1 in Chapter 3 examines and determines legal issues enhancing the development of the effectiveness of law implementation within Thailand's Legal Framework. This perception would involve conducting in-depth studies and providing tentative recommendations and plausible solutions, based on the assessment of Legal Measures. In line with the previous discussion, the resultant addressed perceptions through the enactment of law implementation. This move emphasized the ineffectiveness of law enforcement under Thailand's CCA framework, specifically on the pre-full enforcement of Thailand's PDPA and the repercussions of amendments of the second revision of Thailand's CCA in 2017. The legislation as summarized in that table demonstrates that Thailand's legal framework improved significantly in response to personal data breach incidents with the upcoming enforcement of the PDPA and CSA in 2022. In 2023, Thailand's legal measures were promulgated to enhance security systems, notify authorities of incidents, and enforce laws to encounter, manage, and prosecute offenders in court.

The summarized table illustrates how Thailand's legal framework benefits from the PDPA's comprehensive measures, including but not limited to, compliance duties covering a wider range of scope, implementing security systems, possessing a Data Breach Notifications Law, and offering plausible solutions through dual complaint mechanisms until enactment of PDPC Thailand. Furthermore, it also outlines the process of directing lawsuits to court with various categories of sanctions. As stated by

Graham Greenleaf in *Privacy Law and Business International Report*, Thailand's legislation ensures the effectiveness of legal structures in protecting personal data.¹ This meticulous milestone is achieved through a personal data protection bill explicitly based on the EUGDPR, effective ever since the inception of the official gazette of the PDPA. Thailand's approach to legislative enactments is explained through utilizing the "Legal Transplant" process. PDPA illustrates the specific proceedings and unique interpretations under Personal Data, that includes legal measures for prevention and addresses the organization's and the affected person's approach and recovery by elaborating on organization, technical, and physical measures in the mentioned subordinate legislation demonstration.² Nevertheless, the combination of Thailand's PDPA and CSA Thailand's legal structure, including the CCA and the Penal Code, depicts several drawbacks.

4.1.1 Legal Implementation Issues

This dissertation highlighted a key aspect regarding the classification and regulation of personal data breach incidents, emphasizing that they are legal procedures outlined in subordinate legislation. This adjunction of legislation will serve as a supporting role to provide further clarification and address the gaps in the interpretation and application of the law. The challenge is exacerbated through verification of the details of this secondary legislation (The regulation which is lower than Act, Royal Decree) as

¹ Graham Greenleaf, "Law Comment- From Thailand to Jersey – GDPR's Global Effect is Evident", *Privacy Law and Business International Report*, (2019): 1–6. Privacy Law and Business, via Privacy Law and Business, www.privacylaws.com

² Thailand National Cyber Security Agency, "Annual Report 2023 : Thailand National Cyber Academy (TNCA)", Thailand National Cyber Security Agency official website, <https://ncsa.or.th/Ebook_%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%88%E0%B8%B3%E0%B8%9B%E0%B8%B5%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A%202566.html> (accessed 15 April 2024).

outlined in section 84 (1) of Thailand's Civil Procedures Code.³, which states that the court's investigation of facts must be based on corroborative evidence, except for well-established facts. The Act, Royal Decree, and primary statutes are widely recognized as the "General known" and are not considered a legal interpretation problem issue during court examination. The court ruling from the Official Law Report number 214/2498 (1955) and 256/2516 (1973) emphasized the importance of law reforms, stating that it applies to municipal regulations, government decisions, international law, and regulations that fall under the jurisdiction of the ministry level. It is imperative to observe that parties involved in a dispute should not advocate concerns with the due diligence of the court devoid of explicit claims instructed to be addressed or enactments in line with the according to regulations.⁴ Official law report number 650/2532 (1989) declared that in cases where the plaintiff fails to provide evidence of interest calculation beyond the benchmark, the calculation of damages should adhere to the general provisions outlined in the CCC.⁵

4.1.2 The legal issues on Thailand's Personal Data Protection Act and Cybersecurity Act implementation.

These samples of official law reports address the expected interpretation issues related to the subordinate legislation, stipulate the explanation of the discretionary processes and the details of appropriate security measures under PDPA section 37 (1).⁶ Also, the data breach notification process in the PDPA section 37 (4) regulates the details in the

³ Government Gazette, Thailand Civil Procedure Code.(Volume 134) (Chapter 69 Gor) (Revised 2017). Section 84/1: "the investigation on the fact by the court shall rely on the evidence excepted (1) these fact concerned as the generally known."

⁴ Court of Justice of Thailand, Thailand's Official Law Reports in Data Breach Case (Non-translation).<http://www.supremedekacourt.co.th> (Accessed 15 April 2024).

⁵ Ibid. If the parties cannot uphold the mentioned regulation, the judiciary is concerned as the parties' justification is void, which affects the judiciary's dismissal of the case.

⁶ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Section 37 (1)

subordinate legislation.⁷ Moreover, this substantive, albeit subordinate legislation neglects to prove and illustrate the process. In that case, the outcome and the success of specific amendments such as the PDPA and the CSA shall remain ineffective due to the absence of corroborative evidence in the practical cases, circumvention caused due to abstinence to compliance under the purview of Section 84 (1) of CPC, and the court annulled the case. Thus, these issues should be highlighted among legal practitioners to exercise substantive regulation in the adequate practice of personal data breach cases.⁸

The law reports focus on the glitches associated with legal implementation, when the majority personal data breach incidents, require regulations tantamount to notification by the PDPC, NCSC, or NCRC, as discussed in the previous chapter. Most of the enactments are regulated under Ministry DE regulation, which is concerned with further explanation of amendments from the PDPA and CSA.⁹ Legal practitioners are responsible for ensuring that the "standard" meets regulatory standards, whether by confronting the general requirements or demonstrating exemption from responsibilities. The PDPA, CSA, and CCA were initially identified as the specific issues on legal exercise that require expertise to explain the technical proceedings to the court during cross-examinations. In future legal processes and applications, the expertise, particularly the "Expert witness," specifically the Forensic experts and the specific legal practitioners on the CCA, PDPA, and CSA will play the role significantly into illustrate

⁷ Government Gazette, The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update: March 2024. Such as Notification by PDPC Thailand's proceedings of Data Breach Notification. (Volume 139) (Special Chapter 292 Ngor), Date Enacted: 15 December 2022

⁸ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024. CSA practitioners foresee this practical law implementation in the court procedures, which might occur when the lawsuit combines CCA, CSA, and PDPA, each of which has specific proceedings in technical terms.

⁹ Thailand's Ministry of Digital Economy and Society. (MDES) and Government Gazette. The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (DE) Last update March 2024 (2024). <https://www.mdes.go.th/law> (accessed 15 April 2024)

evidences in the legal proceedings.¹⁰ In the legal practice concerning the detailed in the preceding chapter (case number 2600/2563), the expert witness provided a phenomenal opinion to substantiate the defendant's unauthorized access conduct, thereby satisfying the code of the accusation (Unauthorized Access criminal offence under Sections 5 and 7 of the CCA, as clarified).¹¹

According to the discussion previously in the practice of proof of the PDPA and CSA technical proceedings under the procedures law (Section 84/1 of CPC), Thailand's legal practitioners are responsible for proving the legal requirements and standards and providing specific legal opinions on court proceedings. Through the promulgation of amendment components, expert witnesses shall play an imperative role in providing details and precise proceedings under the guaranteed stipulations of the PDPA, CSA, and the CCA, which require expertise and professional personnel, especially officers, to enhance the law implementations.¹² Moreover, the all legal practitioners under CCA, CSA, PDPA should be sophisticated on their fields in ensuring that the legal requirements are satisfied in preparing litigation expertise to manage personal data breaches and cyber threats.

Furthermore, the outcome of the summarized legislation table identifies a significant paradox related to the overlapping between Thailand's PDPA and CSA

¹⁰ Government Gazette, Thailand's Criminal Procedure Code, (1934).(Volume 136) (Chapter 34 Gor) (Revised 2019), Section 243-244/1 Section 243: The expert witness shall mean a professional who is fluent in a specific skill, such as a doctor, scientist, or international law. Expert Witness may appointed by the parties requesting permission from the court, or the court may consider and appoint in the necessary reasoning. During the testimony or witness examination, the Expert witness may conduct in verbal or written documents.

¹¹ Government Gazette, Thailand Personal Data Protection Act 2019. (Volume.136) (Chapter 69 Gor), Moreover, the Electronic Evidence Act was also implemented through the matters of Illegal Access offences.

¹² General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya", Bangkok, 14 May 2024, PDPA practitioners addressed that Thailand is still in the early enforcement of PDPA and CSA, which still lacks professionalism in these mentioned regulations practitioners. It is believed that the appropriate professional shall enhance Thailand's PDPA implementation comprehensively.

framework in the context of personal data breach incidents.¹³ This paradox involves a wide range of potential conflicts regarding the Data Controller, Data Processors, and Government Agencies and their obligations under the Data Breach Notification Law in Thailand's CSA and PDPA. Government agencies will be liable under the purview of this law if negligence prevails through non-compliance with a regulation. Albeit principles indicate that legislation holds a distinct goal, and their enactment structures should cease to overlap.¹⁴ This issue should be addressed the explicit differentiate for accurate compliance between CSA and PDPA, especially with the Data Breach Notification Law in PDPA Section 37 (4) and the subsequent Section 57 of the CSA Section 57 (Reporting the Cyberthreats incidents to the authority). Therefore, it is recommended that the "Notification Law" be promptly adhered to in the event of a personal data breach. The legislator should establish a specific principle for government entities introduced to the public sectors and the CII units by the implementation of both the PDPA and CSA, mandating concurrent compliance with the notification law for the authorities. This approach would effectively distinguish the compliance responsibility from the two legislations.¹⁵

¹³ The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update March 2024. "Notification of PDPC Thailand's 2022: The principle of data breach notification,(Volume 139) (Special Chapter 292 Ngor), Date Enacted: 15 December 2022", "Notification of PDPC Thailand's 2023: the fundamental standard of the security system of data controller who got the exemption under Thailand's PDPA (Volume 140) (Special Chapter 309 Ngor) Date Enacted: 8 December 2023"

¹³ Annual Report 2023 by Thailand National Cyber Academy (TNCA)."

¹⁴ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024, PDPC authority is concerned that PDPA principles carry the specific regulation and differentiate the complaint and the proceedings of PDPC authority only in PDPA. Thus, even though some principles, such as the Data Breach Notifications Law, shall occur in PDPA and CSA, these principles shall play different purposes and different sanctions, which still do not overlap each other.

¹⁵ The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update March 2024. subordinate legislation under Notification by PDPC Thailand (The processing of Data Breach Notification)(Volume 139) (Special Chapter 292 Ngor), Date Enacted: 15 December 2022, Notification number 4

4.1.3 The Legal issues on the lack of procedure under administrative court dealing with Data Breach appeal and the special court division.

The table in Chapter 3 demonstrates that "Administrative Liability" and the majority of law enforcement, whether under the purview of CCA, CSA, or PDPA framework, primarily involve specific authorities in Administrative Action, Administrative Order, and Administrative Sanction.¹⁶ This phenomenon influences the contextualization of the EUGDPR methodology into Thailand's PDPA and CSA, as well as CCA. The sanction and implementation under the administrative law principle aims to enhance the effectiveness of law implementation within the public sector. The lawsuits from ordinary individuals may not be practical or effective for addressing compliance duties, as Data Subjects solely cannot be relied upon to address and file cases in court.¹⁷ Moreover, the structures of "Administrative law," including substantive and procedural law, are enacted in stark contrast to the judiciary in interpreting and applying the law. The overlap between authorities, administrative liabilities, established orders, and other factors should be considered in the event of a personal data breach. Hence, it is advisable to do in-depth research regarding these Administrative Sanctions and procedures, enhancing to a degree while addressing any potential issues, whether overlapping between the authorities such as PDPC, government practitioners, and the judiciary. The administrative order for promulgation and the practical legal exercise in lieu of stipulated specific sanctions in line with the interpretation and application of these laws.¹⁸

¹⁶ Government Gazette, Administrative Procedure Act, B.E. 2539, (Volume 136) (Chapter 69 Gor) (Revised 2019).

¹⁷ Government Gazette, Act on Establishment of Administrative Court and Administrative Court Procedure, B.E. 2542 (1999), (Volume 116) (Chapter 49 Gor).

¹⁸ Government Gazette, Administrative Procedure Act, B.E. 2539, (Volume 136) (Chapter 69 Gor) (Revised 2019). "Section 48: Administrative orders issued by various committees, whether established by law or not, allow the parties involved to dispute the matter before the Committee for the Consideration

The summary table in Chapter 3 illustrates that various laws and penalties can lead to issues with "Court Jurisdiction" because civil liabilities and criminal liabilities fall under the jurisdiction of the Court of Justice, while administrative matters are under the jurisdiction of the Administrative Court.¹⁹ The responsibility for this criminal act lies with the prerogative of the Criminal Court, but its effectiveness appears to be lacking in the primary legal exercise based on the CCA amendment, as elaborated earlier.

In February 2022, the Court of Justice officially announced the establishment of the "E-commerce Court division" as a milestone.²⁰ This division will manage e-commerce and online purchasing contracts, except cybercrime issues. In April 2024, the Court of Justice officially declared and gazetted the "Cybercrime Division Court"

of Complaints under the law governing the Council of State, both on factual and legal issues, within ninety days from the date of receiving the notice of the order. However, if such a committee is a dispute resolution committee, the right to appeal and the timeframe for the appeal shall be in accordance with the provisions of the law governing the Council of State.” Regarding the administrative principle, PDPC statement authority is the administrative order which if the parties would like to appeal must comply under the Administrative Procedures Act. Moreover, any conflict after the appeal of such an administrative order is under the jurisdiction of Administrative Court.

¹⁹ Government Gazette, Act on establishment of Administrative Court and Administrative Court Procedure, B.E. 2542 (1999).(Volume 116) (Chapter 49 Gor). Section 9““The Administrative Court has the authority to consider, adjudicate, or issue orders on the following matters:

- (1) Disputes regarding actions taken by an administrative agency or government official that are unlawful, whether it involves issuing regulations, orders, or any other actions due to acting without authority, exceeding authority, not complying with the law, failing to follow the prescribed procedures, or failing to act in good faith, engaging in unfair discrimination, creating unnecessary procedures, or imposing unreasonable burdens on the public, or exercising discretion improperly.
 - (2) Disputes regarding the failure of an administrative agency or government official to perform their duties as required by law or performing such duties with unreasonable delay.
 - (3) Disputes regarding tortious acts or other liabilities of an administrative agency or government official arising from the exercise of legal authority, from regulations, administrative orders, or other orders, or from failing to perform duties as required by law or performing such duties with unreasonable delay.”
- Thus, PDPA administrative liability is under the jurisdiction of the Administrative court. Meanwhile, the Court of Justice's jurisdiction is responsible under the Civil and Criminal liability of the PDPA.

²⁰ Thailand’s Court of Justice, "D-Day Court of Justice Declared the Opening of E-Commerce Special Division Operations under Civil Court Division. Court of Justice Spokesman Emphasised that the 24-Hour Filing also Available with the Slogan [the Justice is Easily Accessible]”, Thailand’s Court of Justice official website, 2024, 2022, February 1. <https://www.coj.go.th/th/content/category/detail/id/8/iid/278977> (Accessed 15 April 2024)

formation, subliming to a genuine benchmark.²¹ Cybercrime issues from Thailand's PDPA, CSA, or CCA are expected to be consolidated under this division. Precise measures are expected to be incorporated, ensuring they be taken to ensure fair trials with adequate procedures for all litigants. Thailand is enhancing its legal framework by conducting detailed studies to update and streamline the Procedure Law. This effort aims to centralize the resolution of disputes related to Cyber Law within the existing legislation, similar to Thailand's Intellectual Property²² and Consumer Protection frameworks.²³ The goal is to improve efficiency and reduce conflicts between different laws.

4.1.4 Non- Effectiveness of the legal provisions regarding personal data breach

Conclusively, this study established genuine links between substantive and procedure enactments that could enhance the effectiveness of law through the application of civil liability under Thailand's PDPA and CCC regarding compensation and remedy matters.²⁴ Significantly, personal data breaches usually caused widespread harm and numerous victims. Therefore, the fruitful procedures principle of "Class Action" could be implemented in the legal exercise.²⁵ According to the Class Action

²¹ Thailand's Court of Justice, (Thailand's Court of Justice Officially Established the Cybercrime Division)", Thailand's Court of Justice official website, 2024, April 3. <https://www.coj.go.th/th/content/category/detail/id/8/iid/407872> (Accessed 15 April 2024)

²² Act for the Establishment of and Procedure for Intellectual Property and International Trade Court.(Volume 139) (Chapter 32 Gor) (Revised 2022).

²³ Government Gazette, Thailand Consumer Protection Act BE2551 (2008),(Volume 125) (Chapter 38 Gor).

²⁴ Theerachit Jitkarunawong, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act And EU's General Data Protection Regulation (EUGDPR)", (Unpublished Master's. Independent Study Dissertation, Thammasart University, 2019).

²⁵ Government Gazette, Thailand Civil Procedure Code. (Volume 134) (Chapter 69 Gor) (Revised 2017). Section 222/14-222/34

Section 222/29 During the court examination in the class action case, the court may grant permission for parties to settle the dispute by negotiating at any time before the examination is finished. Section 222/30 During the court examination, the court may grant permission for parties to settle disputes by an arbitrator, but the procedures shall not contrast with the principle in section 222/29.

principle, it is expected that the injured shall receive the appropriate compensation inclusively in terms of amount, and this principle may shorten the duration of procedures²⁶. The personal data breach event, which initially harmed society at a larger scale, causing catastrophic victimization to data-owners persons, is anticipated under this principle to grant compensation. The remedy will cover damages for data subjects as injured persons in terms of quantities.²⁷ However, the context of personal data breaches is still new and lacks a legislative implementation sample. Thus, it is recommended that in-depth studies are conducted through legal research regarding the compensations provided in personal data breach incidents.²⁸

Through Sections 44/1 to 44/3 of Thailand's Criminal Procedure Code, it establishes the critical notion of the special request for compensation in criminal cases where the public prosecutor, acts as the plaintiff. This principle directly enrooted through a combination, varying through criminal and tort law to civil law.²⁹ The principle of unique compensation requests can demonstrate the efficiency of combining criminal procedures and granting compensation, thus expediting the completion of trial cases by simultaneously pursuing them in criminal and civil courts. This is particularly relevant in personal data breach cases involving direct criminal liability under precedents enshrined in laws such as the CCA, CSA, or PDPA. Thus, in practical cases

²⁶ Ibid. Section 222/20 During the court examination, the court may appoint the exact duration for the trial of the class action case. Moreover, the court may conduct the witness examination and evidence investigation briefly and determine under the necessary cause and justice reasoning.

²⁷ Richie, J. Thomas. 2015. "Tort Trail and Insurance Practice: Data Breach Class Actions." *GPSolo* 32 (No. 5): 66–67. JSTOR, via JSTOR, <https://www.jstor.org/stable/24634368>.

²⁸ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024. As the representative of the private sector, Dr. Udomtipok emphasized the class action principle, which may be fruitful when applied under personal data breach circumstances. This tool shall enhance the injured person requesting compensation from the data controller or perpetrators. Also, with the grouping of parties in terms of class action, the court may provide compensation comprehensively than usual, pliant the lawsuit based on the normal civil case under PDPA and CCC. However, PDPA is still in the early enforcement duration that requires in-depth studies of how the class action principle may be applied in the context of personal data breaches.

²⁹ Government Gazette, Thailand's Criminal Procedure Code. (Volume 136) (Chapter 34 Gor) (Revised 2019), Section 44/1

such as CSA and the PDPA criminal liability, the data subject or injured person in a personal data breach can utilize these tools to seek redress from the defendant through court application for an inclusive and suitable remedy. In addition, the CSA and the PDPA structure have implemented the "Corporate Veil" notion, as discussed in the previous chapter.³⁰ Therefore, as a legal entity, the defendant can be held accountable for criminal acts under the application of this law.

Section 44/1 of Thailand's Criminal Procedure Code impacts the successful implementation of the law in criminal and tort law cases. Class action and distinctive compensation requests in criminal cases should be overseen according to the existing legal mechanisms within Thailand's legal system. The victim must play a supporting role in the criminal procedure trial alongside the public prosecutor, who is the prime plaintiff, ensuring the appropriateness of treatment and enhancing the trial's effectiveness in the personal data breach event.³¹

Thailand's legal framework incorporates commendable, albeit comprehensive measures derived from the original EUGDPR³², as enriched in the model outlined in the PDPA legislation.³³ The complex compliance obligations involve a multi-layer process for reporting complaints with the PDPC Thailand, through various categories of

³⁰ Thawat Buapitak Vice presiding Judge of Udon Thani Provincial Court, "The Principle of Piercing the Corporate Veil with Consumer Protection", *Official Court of Justice articles COJ library*, via Court of Justice library, <https://library.coj.go.th/pdf-view.html?fid=51341&table=files_biblio>. (Accessed 15 April 2024).

³¹ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024. CSA practitioners emphasized that most legal execution is based on CCA, while PDPA and CSA carry the criminal sanction just enforced. Section 44/1 of CRPC may be of benefit in the personal data breach case. This principle shall provide the shortcut to requesting compensation in the criminal case, which shortens the duration of legal proceedings. However, PDPA and CSA are still in early enforcement. This issue should be addressed so that in-depth studies continue to enhance the effectiveness of law implementation.

³² 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.) <https://gdpr-info.eu/>

³³ Government Gazette, Thailand Personal Data Protection Act 2019, (Volume.136) (Chapter 69 Gor).

sanctions to ensure the overall protection of personal data and prevent data compromise.³⁴ Furthermore, Thailand's CSA and the CCA were amended twice through the efforts of legislators, enabling legal measures and fundamental ICT-(Information Communication and Technology) crimes. The primary influence is deduced from the Penal Code and the CCC, which jointly establish liability for physical criminal offences and provide additional compensation for damages claimed through courts.³⁵ The assessment could examine many aspects of law implementation under the present procedure law, focusing on specific principles, particularly in administrative law, that may encounter new obstacles. The assessment could examine many aspects of law enactments under the present procedure law, focusing on specific principles, including but not limited to particularly in administrative law, that encounter new obstacles. Hence, these assessment opinions enable recommendations and suggestions enhancing Thailand's legal framework to enhance the through effectiveness of legal measures in dealing with personal data breach incidents and other cybercrime and cyber threat events.

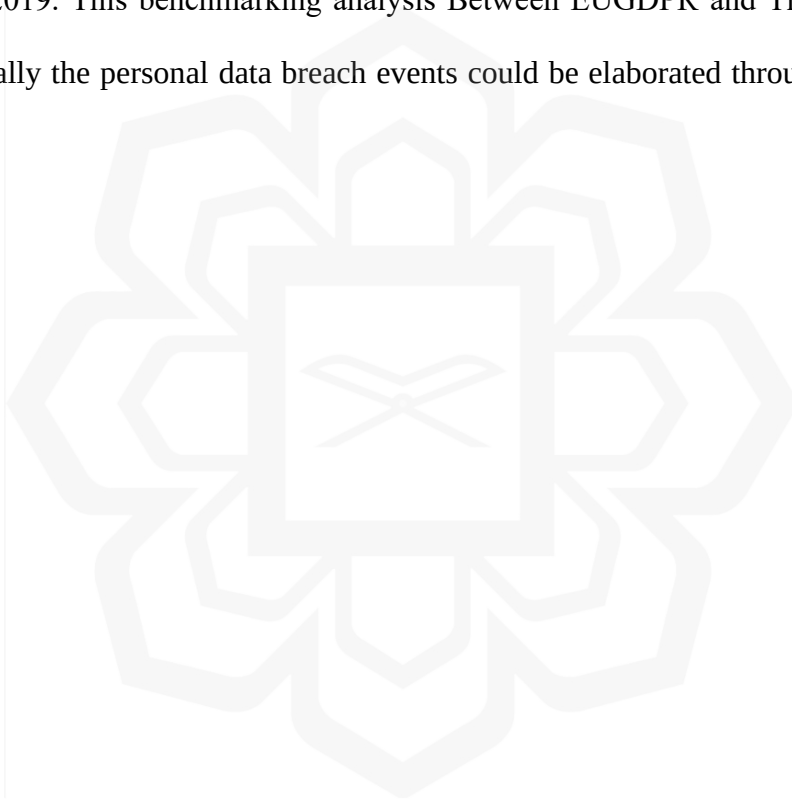
Through this internal assessment of Thailand's Legal Framework, this thesis will establish a benchmark primarily anticipating an effective role of Thailand's PDPA 2019 with the enactment of the European Union General Data Protection Regulation (EUGDPR) 2016. The benchmark analysis provides findings, comments, and other suggestions to improve the effectiveness of Thailand's legal interpretations and implementation in the event of personal data breaches.

³⁴ Ibid.

³⁵ Theerachit, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act and EU's General Data Protection Regulation (EUGDPR)" ...,39-41.

4.2 THE BENCHMARKING ANALYSIS: EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (EUGDPR) AND THAILAND'S PERSONAL DATA PROTECTION ACT (PDPA) 2019

From the previous chapter, this dissertation mentioned the phenomenon of “Legal Transplant”³⁶ through the primary legislation as the European Union General Data Protection Regulation (EUGDPR), which upholds physical privacy aligned with the let alone theorem into information privacy establishing data subject rights. After the EUGDPR effective regulation in 2018, Thailand completed the enactment of Thailand's PDPA 2019. This benchmarking analysis Between EUGDPR and Thailand's PDPA, specifically the personal data breach events could be elaborated through this Table as follows;



³⁶ Alan Watson. 1996. “Aspects of Reception of Law.” *The American Journal of Comparative Law* 44 (2): 335. Heinonline, via Heinonline, <https://doi.org/10.2307/840712>.

Table 4.1 The benchmarking Analysis Between Thailand's Personal Data Protection Act 2019 and the European Union General Data Protection Regulation 2016 in the Personal Data Breach event on the legal arrangements.

Salient Features	European Union General Data Protection Regulation 2016	Thailand's Personal Data Protection Act 2019	The Availability of legal measures
Definition of Personal Data Breach	Article 4 (12)	subordinate legislation under Notification by PDPC Thailand's (The processing of Data Breach Notification) section 3	Both EUGDPR and Thailand's PDPA enacted the stipulated legislation. However, Thailand's PDPA explicitly defined personal data breach in the subordinate legislation.
Compliance duty to provide the appropriate security system	Article 32	Section 37 (1), subordinate legislation under Notification by PDPC Thailand's (The security standard for Data Controllers) Section 4	Both EUGDPR and Thailand's PDPA promulgated this stipulated regulation. Thailand's legal framework laid down tentative principles for PDPA and expansion of elaborations through subordinate legislations.
Compliance duty to provide the Data Privacy Impact Assessment (DPIA)	Article 35	Section 37 (1), 39 (8), 40 (2), subordinate legislation under Notification by PDPC Thailand's (The security standard for Data Controllers) Section 4	Both EUGDPR and Thailand's PDPA implemented the stipulated regulation. Thailand's PDPA continues to expand the explanation of the subordinate legislation. Moreover, This duty explicitly differentiates from the CSA framework.
Duty of Data Breach Notification	Articles 33 and 34	Section 37 (4), subordinate legislation under Notification by PDPC Thailand's (The processing of Data Breach Notification) Section 4	Both EUGDPR and Thailand's PDPA implemented the regulation mentioned. Thailand's PDPA continues to expand the explanation of the subordinate legislation. Moreover, This duty explicitly differentiates from the CSA framework.
The complaint functions through the supervision/ authorities organisation.	Articles 77 -80	Chapter 5 of Thailand's PDPA (Section 71-76) and the guideline to specify the	Both EUGDPR and Thailand's PDPA implemented the stipulated regulation. Thailand's legal framework specifically regulates confrontation procedures based on Thai administrative law principles.

		administrative liability in Section 90 of Thailand's PDPA	
Civil Liability	Article 82	-Section 77, the general actual damages -Section 78 of the punitive sanction	Both EUGDPR and Thailand's PDPA implemented the stipulated regulation. Thailand's legal framework divided the liabilities into two main basis.
Criminal Liability	Article 10	Sections 79-81	Both EUGDPR and Thailand's PDPA implemented the stipulated regulation. The authority under the European Union member state criminal convictions state regulates EUGDPR. Simultaneously, Thailand's Legal Framework regulated specific criminal liabilities.
Administrative Liability	Articles 83, 84	-Section 83 (Data Controller) -Section 86 (Data Processor) -The specific guideline to specify the sanction Section 90, subordinate legislation under Notification by PDPC Thailand's (The direction into appointed the PDPA's administrative sanctions) section 3 and 8	Both EUGDPR and Thailand's PDPA implemented the stipulated regulation. Thailand's legal framework continues elaborating on the subordinate legislation's details.
Supervisory authority	Chapter 6 and Chapter 10 of EUGDPR (Sections 51-59 and 92-93)	Thailand's PDPA Chapter 1 (Section 8-18)	Both EUGDPR and Thailand's PDPA implemented stipulated regulation. Thailand's legal framework addressed the authority devoid of any extra-territorial effect.

From the summarization table, the principles that Thailand's PDPA adopted from the EUGDPR are mentioned as follows:

1. Definition of Personal Data Breach
2. Duty to provide appropriate security system
3. Duty to undertake the Data Privacy Impact Assessment (DPIA)

4. Compliance duties following the Data Breach Notification Law
5. The complaint functions through the supervision/ authority's organization,
6. The sanctioned categories are Civil, and Administrative Non-Compliance Liabilities, and
7. Supervision authority units under regulation.

From the adaptation and contextualization principles, it could be illustrated that Thailand's legal framework awareness of the upcoming principle is expected to be one of the factors that Thailand's legal framework adopted due to the influences of Cross-Border Data Transfer principles.³⁷ The effect is recognized globally in the sense that under mitigating circumstances if Thailand could not provide appropriate personal data protection framework, international cooperation on personal data processing with international parties might not be comprehensively provided in accordance with international best practices. Hence, circumventing corporate progress, business would be interrupted.

Firstly, regarding the definition of a personal data breach. Thailand's subordinate legislation under the purview of Thailand's legal framework has provided detailed principles beyond the primary Royal Decree and legal statutes as demonstrated in the previous chapter. The table and analysis by Kanathip revealed that the "personal data breach" concept in EUGDPR should encompass "accidental circumstances,"³⁸ a scope more extensive than that of Thailand's legal framework, which does not include provisions for data breach scenarios. Thailand's legal framework criminalized "Intention to commit Illegal Access" under Thailand's Computer Crime Act. Through

³⁷ Kanathip Thongveerawong, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, (Thailand: Nitithamlawbooks, 3rd edn., 2022), 64-65.

³⁸ European Union General Data Protection Regulations. Article 4 (12) personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

interpretation of the law, there may be subtle discrepancies in how the personal data protection framework and the EUGDPR are legally analysed, with the EUGDPR comprehensively interpreted. The Notification of the PDPC Thailand defines personal data breach as negligence that may lead to accidental circumstances.³⁹ Thus, Thailand's legal structure included the prototype notion of compliance duty straight into the PDPA. It further expanded regulation under the CSA framework outlined in the preceding chapter.⁴⁰

Secondly, the legislation outlines compliance obligations regarding the security systems approach. Thailand has expanded the scope of the application of security standards principally in the subordinate laws outlined in the preceding section. The EUGDPR and the PDPA 2019 have distinctive similarities as both enactments are regulated through tentative content. However, EUGDPR laid down this principle in detail⁴¹ exclusively through Section 37 (1) of the PDPA 2019, which focuses on the CIA principles, the code of conduct in Article 40, and the Certification of the appropriate security system in Article 42.⁴² The overall details of these features of the

³⁹ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 372-373. The author interpreted this issue as personal data breaches, mainly based on the interpretation of unauthorised access in the CCA framework. Therefore, it is determined that Thailand's judiciary should interpret this incident based on CCA's background. However, the definition of notification by Thailand's PDPC personal data breach includes accidental reasoning.

⁴⁰ The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update: March 2024. Notification by NCSC: The appropriate standard of cybersecurity for the information or internal cyber system 2023" Notification by PDPC Thailand's the processing of data breach notification number 4

⁴¹ European Union General Data Protection Regulations. Article 32 (1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (the detail elaborated under (a)- (d))

⁴² Ibid. Article 32 (3)

PDPA 2019 uphold the overall principle applicable in the Notification by PDPC Thailand, which is enforced following the main enactment of the PDPA in 2022.⁴³

Thirdly, due diligence applies imperatively vide the distinctive features of the DPIA (Data Privacy Impact Assessments). EUGDPR upholds this feature as one of the flagship principles detailed in Article 35. This feature highlights the appointment of the imperative personnel of the DPO (Data Protection Officer), who are supervised under authority, and the regulatory statutes through the application of these features.⁴⁴ Meanwhile, the PDPA 2019 principle did not explicitly mention this provision. Nevertheless, DPIA stipulated subordinate legislation and considered through extended elaboration of Section 37 (1) of the PDPA 2019.⁴⁵ Moreover, this principle expanded in Thailand's CSA framework, as the primary legal measure for encountering cyber threats, especially personal data breach incidents, as the "Pre-Risk Assessment" measure, bound to act immediately when observing a data breach. Rest assured, the DPIA will assist alongside the appropriate security measures for the prevention, detection, suppression, and recovery of personal data breach incidents implemented under Thailand's Legal Framework strategies in PDPA and CSA.⁴⁶

Significantly, the duty of Data Breach Notification from the table illustrates mutual congruency of this notion between both EUGDPR and PDPA 2019. Moreover, the original EUGDPR regulation carried the enactment's conclusive definition of Notification regulation.⁴⁷ Hitherto, Thailand's legal contextualization expanded the

⁴³ The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update: March 2024. Notification by PDPC Thailand, the standard of security system section 4.

⁴⁴ European Union General Data Protection Regulations. Article 35 (1)- (7).

⁴⁵ The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update: March 2024. Notification by PDPC Thailand, the standard of security system section 4.

⁴⁶ Ibid.

⁴⁷ Narong Jaihar, et al., *General Data Protection Regulation (Thailand's description version)*, (Thailand: T.press Ltd., 4th ed.,2022). Articles 33 and 34

details, standards, categorizes, and authority that responded after been notified by the PDPC Thailand. Furthermore, Thailand's legal framework parallels the drafting and enforcement of the CSA frameworks, and this principle is also adopted in the context of "Cyber Threats" and Critical Information Infrastructure (CII)⁴⁸ enabling protection of the CIA and the Cybersecurity regulations. This contextualization methodology of Thailand's legal framework has contributed internally to both pros and cons. The comprehensive structure of regulations into interpretation and implementation perceives guidelines from international best practices "international standard" with the expansion principle in the CSA framework. This feature is recognized in the wording of Report duty instead of the Data Breach Notification⁴⁹ to set a contrast between proceedings of the PDPA and CSA amendments.⁵⁰

A comparison between EUGDPR and Thailand's PDPA related to civil and administrative liabilities is observed. Both laws hold the Data Controller and Data Processors accountable for Non-Compliance, which can be detrimental to the "Data Subject" or Personal Data owner. Additionally, these laws govern the excessive rates of compensation through punitive measures. The legal framework in Thailand is not typically regulated with higher compensation for damages, as opposed to the (EUGDPR), which grafts legal damages worth ten million Euros and/or 2% of the total worldwide annual turnover.⁵¹ Such a lucrative incentive covers significant damages to expected remedies, whether or not, the recovery is granted through the organization or

⁴⁸ Government Gazette, Thailand Cybersecurity Act 2019.(Volume.136) (Chapter 69 Gor), Sections 56-58.

⁴⁹ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor), Section 37 (4) elaborated in Chapter 3.

⁵⁰ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024. CSA practitioners know this overlapping issue is related to the same features in the two legislations. However, this principle is enforced under the "Report" terms in the CSA framework, which appeared in CSA sections 56-58.

⁵¹ Narong, *General Data Protection Regulation (Thailand's description version)*. Articles 77 and 78

to the claimant. Legislators must consider the punitive measures, resulting from non-compliance, hence ensuring organizations and individuals, adherence to international best practices.⁵² Thailand's Legal Framework introduced Section 78 of the PDPA to litigate Civil Liability related to punitive actions, aligning with the EUGDPR rules, thus utilizing a distinct computation method.⁵³ Thailand's legal system is based on the Civil and Commercial Code (CCC), which serves as the central legislature for tort law and determines compensation in commercial disputes, as decided by the judiciary. Although the legal foundation may significantly vary from the EUGDPR, the result and efficiency of legal enforcement are identical, maintaining quality assurance as mentioned in the CCC and the PDPA.

Meanwhile, Articles 83 and 84 define a broader spectrum of the Administrative sanctions for Non-Compliance in the EUGDPR,⁵⁴ tantamount to Sections 83 and 86 of Thailand's PDPA.⁵⁵ Moreover, Thailand's legal framework is adapted to the principles that shall be investigated and linked to the PDPC authority, including but not limited to the appeal proceedings on administrative law principles, as stipulated in Section 90, followed by subordinate legislation as notified by the PDPC Thailand.⁵⁶ Specifically, DPIA non-compliance and the Joint Controller principle in EUGDPR are provided for.⁵⁷ However, Thailand's legal framework does not recognise this liability. This

⁵² Narong, *General Data Protection Regulation (Thailand's description version)*. Articles 77 and 78

⁵³ Theerachit, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act and EU's General Data Protection Regulation (EUGDPR)".53-55.

⁵⁴ Narong, *General Data Protection Regulation (Thailand's description version)*. Articles 83 and 84 of EUGDPR

⁵⁵ Government Gazette, Thailand Personal Data Protection Act. (Volume.136) (Chapter 69 Gor), Section 90.

⁵⁶ The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update: March 2024. Notification by PDPC Thailand: The main principle into specify administrative order sanction under expert committee (2022)" Notification by PDPC Thailand: The specify administrative order principle (Volume 139) (Special Chapter 140 Ngor) section 3 and 4.

⁵⁷ Narong, *General Data Protection Regulation (Thailand's description version)*. Articles 83 and 84 of EUGDPR

notion is expected to be another effect of the “contextualisation” relating to Thailand's administrative law frameworks. Nevertheless, Thailand’s CSA framework will fill this loophole.⁵⁸ Further in-depth study, specifically on administrative sanctions, is anticipated to lead the scope of the problem statement.

This benchmarking exercise further illustrates the difference in criminal liability.⁵⁹ Thailand's PDPA is determined by adapting and contextualising the EUGDPR methodology⁶⁰, explicitly focusing on the illegal disclosure of personal data, comprised through negligence by data controllers and processors.⁶¹ Furthermore, this criminal liability bridges the gap arising from the liability clause in the Computer Crimes Act and Penal Code⁶², which is an additional obligation. PDPA does not possess any overlap. Moreover, the offender has been broadened under the CSA framework in relation to the Cyber threats scenario, explicitly targeting the Officer under CSA legislation.⁶³ In addition, the actual encounter operation can be observed using the 9-Near⁶⁴ and the JIB Computer.⁶⁵ The criminal sanction⁶⁶ category results from legal procurement and criminalisation, demonstrating an understanding of the loophole in the

⁵⁸ Annual Report 2023 : Thailand National Cyber Academy (TNCA).

⁵⁹ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 518-520.

⁶⁰ European Union General Data Protection Regulations. Section 10 Processing of personal data relating to criminal convictions and offenses, or related security measures based on Article 6 (1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

⁶¹ Government Gazette, Thailand Personal Data Protection Act 2019. (Volume.136) (Chapter 69 Gor). Section 80, described in Chapter 3

⁶² Ibid. Sections 79-81 described in Chapter 3

⁶³ Government Gazette, Thailand Cybersecurity Act 2019. (Volume.136) (Chapter 69 Gor), Sections 70-72.

⁶⁴ *BBC Thai*, 9near : “จับกุม จำคุก โท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว” (9-Near the criminal claimed that hold Thailand's population data for 55 millions records got caught already)., *BBC Thai*, 2023 March 31 <https://www.bbc.com/thai/articles/cq5z3w5lwdxo> (accessed 15 April 2024)

⁶⁵ *Matichon Online*, “JIB” Admitted that the Personal Data Breach had Happened. Thailand’s PDPC is under Investigation for This Fact.” *Matichon Online*, 2024, March 28. https://www.matichon.co.th/economy/news_4498411 (accessed 15 April 2024)

⁶⁶ Government Gazette, Thailand Personal Data Protection Act. (Volume.136) (Chapter 69 Gor), Section 79-81.

CCA framework and the precise application of the legislation circumventing overlap issues. Furthermore, this criminal liability is enshrined within Thailand's internal jurisdiction. Thus, this criminal liability is thought to enhance the efficiency of Thailand's PDPA. A legal framework should be implemented to address and deal with offenders fairly and legally to uphold society's peace, in its genuine form.

Lastly, from the table, similarities are observed between the supervision authorities and the complaint function, through which Thailand's legal framework is aware of the significance of this function and adopted the EUGDPR principles to establish PDPC Thailand. However, the EUGDPR as the rudimentary model legislation has provided regional and internal institutions sufficing ordinary supervision authority to monitor overall personal data activities in compliance with the regulation through the adoption of the "EDPS" (European Data Protection Supervisor) principle. This process supervises the "Internal authorities" to provide guidelines, and to guide the PDPA compliance including but not limited to dispute resolution.⁶⁷ The EUGDPR guided EU member States to adapt and adjust, information privacy principles by expanding its reach throughout the EU region. Regional realm. Thailand is devoid of such a magnanimous scope, as the internal supervision authority is the prerogative of the Ministry of Digital Economy (MDES).⁶⁸ Moreover, their due diligence exhibits similarity to both Thailand's PDPA and the EUGDPR. This authority holds the right to settle disputes under the complaint of the Data Subject into proceeding with any malicious activities, whether committed by the Data Controller or Data Processors,

⁶⁷ Narong, *General Data Protection Regulation (Thailand's description version)*. The EUGDPR's characteristic fines are different from those of PDPA 2019, as EUGDPR is regulated under Art. 83(5) GDPR, the fine framework can be up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year, whichever is higher. Meanwhile, PDPA 2019 regulated the fixed rate of administrative sanctions.

⁶⁸ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 522-525.

including the Non-Compliance activities observed in the case of JIB Computer. Furthermore, the statement by PDPC is limited to specifying the Administrative Non-Compliance Sanctions in the context of the Administrative Order stipulated in Thailand's legal framework, Article 81 to 84 of the EUGDPR.

The issues of supervision authorities, especially the EDPS organisation, Thailand, and ASEAN's focus shall now be on the potential to uphold and address regional cooperation in terms of the personal data protection regional authority. This regional organisation will extend cooperation, conserve time for the dispute proceedings, upholding transparency and fairness compliance of personal data protection principles through achieving centralised and standardised personal data protection regulation. However, establishing regional authorities like EDPS diversifies the legal system, and poses challenges. For instance, Thailand and Indonesia adhere to a Civil Law system, while Malaysia and Singapore inherited a Common Law realm. Therefore, throughout the challenges, through in-depth study of the harmonisation of personal data protection law in ASEAN should be conducted to establish the alternative functional of a personal data protection authority in the ASEAN region.⁶⁹

Indeed, Thailand has already anticipated regional cooperation, through the "ASEAN Digital Masterplan 2025 and Privacy Framework 2016 on Digital Data Governance 2018" and the additional regional framework of "Implementing Guideline for the ASEAN Cross Border Flow Mechanism 2021."⁷⁰ This cooperation was established when Thailand reviewed primary drafts of the PDPA and the CSA 2019. However, with the PDPA and the CSA enforcement, Thailand's legal framework is

⁶⁹ Sonny Zuhuda and Ridoan Karim, *Cyber Law in Malaysia : Principal and Practices*, (Malaysia: Sweet and Maxwell, 2024), 270-271. The author's conclusion on the emphasis of the ASEAN Privacy framework announcing including the ASEAN cross border transfer principles.

⁷⁰ Sonny, *Cyber Law in Malaysia : Principal and Practices*, 164-171.

bound to follow the guidelines and cooperate. The guideline under the regional partnership exemplifies as proof that the phenomenon of legal adaption of the global standard of information privacy as EUGDPR is essential and effective, especially in the cross-order data transfer principle effect. Even though the ASEAN regional partnership primarily focuses on the economic angle, the application of comprehensive personal data protection principles is further highlighted in this cooperation. Therefore, establishing the Regional Supervision Authority as an initiative, following the EUGDPR model, upholds alternative functions for conducive personal data protection measures in the region encompassing effective law implementation.⁷¹

The comparison between Thailand's PDPA 2019 and EUGDPR revealed numerous similarities, with Thailand's legislative framework is developed through the Legal Transplant method.⁷² The approach incorporates both adaptation and contextualisation methods. Significant precincts of the law closely resemble the model. Thailand's Legislature decided to enhance specific procedures and structures addressing issues within Thailand's administration system through the formulation of a supervision authority under the auspices of the Ministry of DE, implementing a complaint function⁷³ insignificant contrast is observed between Thailand's legal system and the EUGDPR. Nevertheless, they still face prototype legislation, incorporating the original legislation regarding punitive sanctions, criminal liabilities, and administrative fines.⁷⁴ Thailand encountered issues causing delays in complete enforcement, starting with the previous

⁷¹ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024. PDPA practitioners addressed this model as adapted and developing further in the ASEAN boundaries, which may start from Thailand, Malaysia, Singapore, and Indonesia and continue to expand to cover all of the countries in ASEAN. Moreover, the PDPC authority emphasized further studies of the Harmonization of Personal Data Protection Law in ASEAN boundaries. It is believed that regional authority shall benefit the regional cooperation comprehensively.

⁷² Alan, Aspects of Reception of Law.

⁷³ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 522-529.

⁷⁴ Graham, Law Comment-From Thailand to Jersey – GDPR's Global Effect is Evident., 3-6.

chapter. Comparing the benchmarking analysis with Thailand's Legal framework assessment revealed advantages and disadvantages. This comparison offered valuable recommendations for further developments of Thailand's legal framework to ensure high-quality standards through effective legal measures in dealing with personal data protection issues and personal data breach circumstances on internal, regional, and global levels.

Based on this analysis, in the next section, the research will now mold toward global issues playing significant roles in the personal data breach circumstances, alluding to “Artificial Intelligence”.

4.3 THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE PERSONAL DATA BREACH

Artificial Intelligence started to develop significantly since 2016. This development could be seen that this technology has grown virtually through the advancement of technology of the internet, computers, and the expansion of cyberspace.⁷⁵ However, the tools and the freedom to access and use it is unavoidable because of tech-savvy personnel, who may carries illegitimate and uphold savage intentions. AI is expanding its reach and scope beyond peripheral boundaries through intensive training. The “Deep Learning” features enhance the effectiveness of certain savage operations.⁷⁶ Pondering upon the plight of data subjects unavoidable factors cause software participation in the accelerated effectiveness of both security and the invasion scheme.

⁷⁵ Carla Lozonschi Irina Bakhaya, "Artificial Intelligence and its Impact on Cybercrime" in *The International Conference on Cybersecurity and Cybercrime 2023 organized by the Romanian Association for Information Security Assurance*, vol. 10 (Bucharest: Publisher, 2023), 120–126. the Large-Language Model (LLM) is functional through deep learning, AI carries unbelievable skills that assist humanity in activities.

⁷⁶ Philip Treleaven, et al., University College London, "The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami", *University College London*, (2023): 1–34. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/372399289_The_Future_of_Cybercrime_AI_and_Emerging_Technologies_Are_Creating_a_Cybercrime_Tsunami. The researchers gather the possible technologies that AI-generated and analyse them with the cybercriminals' operations.

From the elaboration on the nature of personal data breaches, the main element of cyber attacks could be unauthorised access, as the primary objective component prior to compromised personal data. Artificial intelligence capabilities tremendously assist in generating multiple data of variable types. Thus, the relationship between AI and personal data breach is tantamount to that of dynamite and fire, alluding to cybercrimes. Mostly, the role of virtual software is critical in obtaining compromised personal data. Therefore, the elaboration of AI assistance's role in enhancing the effectiveness of personal data breach has reached a quantum leap in recent years, especially post-introduction of Chat Bots, metaverse, and fintech technologies.

Primarily, in terms of unauthorised access, cybercriminals are concerned with factors targeting the vulnerable systems; alluding to the potential of AI.⁷⁷ Therefore, it is undeniable that Artificial Intelligence possesses high processing integrity skills⁷⁸. Moreover, because of training, the research studies demonstrated that generative AI could identify the user's password with 95% accuracy. Through results of studies, it determines the tech-savvy attributes of cybercriminals as well-versed in computer science and technology, such as AI itself, applying their skills in personal data breaches.⁷⁹ From this high accuracy generative and if it is effectively under-implemented, cybercriminals may unlock access to sensitive data, through the database easily. Furthermore, by virtue of unauthorised access, cybercriminals calculate perfect timing until the victim's security system is activated. Amazingly, the upcoming high-

⁷⁷ Philip , The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami",1–34. LLM mainly training to response the instructions prompted through the feeding large scales of information as Big Data.

⁷⁸ Tais Fernanda Blauth, et al, "Artificial Intelligence Crime: an Overview of Malicious Use and Abuse of AI", *IEEE Access*, vol. 10 (2022): 77110–77122. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/362096921_Artificial_Intelligence_Crime_An_Overview_of_Malicious_Use_and_Abuse_of_AI

⁷⁹ NewsNation, "Study: AI can Steal Passwords with 95% Accuracy", <<https://www.newsnationnow.com/business/tech/study-ai-steal-passwords-95-percent-accuracy/>> (accessed 2 April 2024).

accuracy evaluation of AI decreases the processing time in the first phase of this cybercrime and could launch the invasion, exposing sensitive information through cracking passwords of the encryption of the security system or the administrator's system access account. Nevertheless, this feature might be unsuccessful if the database security system holds double-authentication techniques or multi-layers, for verification purposes, thwarting access to the database.⁸⁰

Secondly, AI demonstrates significant features of generative realms through both pictures and voice. This feature could generate both the image and voice of the target. The research unraveled the chain of unlawful acts by using the obtained information promptly.⁸¹ This AI generative feature creates a new picture and voice, symbolizing "Deepfake."⁸² As this feature is applied to personal data breaches, cybercriminals could have obtained sufficient material collected through open sources of information to train AI and impose the feature of impersonation. Interestingly, this feature could be successful whether applied to sensitive data or biometric data. However, it is difficult to separate a natural person from an impersonator.⁸³ Implementation through deep fake when operating a personal data breach, cybercriminals could impersonate the administrator to gain direct access to the victim's database or still launch these tools to the victim's stakeholders to earn the rights to

⁸⁰ Zahra Hassanzadeh, Robert Biddle, and Sky Marsen, "User Perception of Data Breaches", *IEEE Transactions on Professional Communication*, vol. 64, no. 4 (2021): 374–389. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/356685705_User_Perception_of_Data_Breach_es.

⁸¹ Philip, The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami.1–34. The details of illegitimate generative the study illustrate in terms of "Deepfake".

⁸² Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024. CSA practitioners emphasized that most identity theft is conducted through AI generative features.

⁸³ Xichen Zhang, et al, "Data breach: Analysis, Countermeasures and Challenges", *Int. J. Information and Computer Security*, vol. 19 (2022): 402–442. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/365721658_Data_breach_analysis_countermeasures_and_challenges.

access the targeted more efficiently yet decrease the operational time.⁸⁴ In short, such AI-generative features launched in the cybercrime scheme include personal data breaches. However, in Thailand, most of these malicious activities were used in committing crimes of Identity Theft, Online Fraud, and scams, more than personal data breaches.⁸⁵ Yet, this feature plays an essential role in assisting the succession of unauthorised access and obtaining the personal data in the victim's storage oblivious to scamming.

Thirdly, as mentioned above, in the distinctive processing of personal data breaches, cybercriminals impose “multiple cybercrimes”, demonstrated through the malicious software. The software increases the successful rate of illegally obtaining personal data.⁸⁶ The advancement of AI capabilities through malwares exposed the security system to vulnerability, defecting the entire portal significantly. Moreover, malware could be used in “ransomware”, when applied, can disrupt and compromise the security system to be vulnerable and lock the access gateway to bargain and exchange money or personal data. This invasion could be examined from the circumstances of “Malwarebytes”.⁸⁷ It is beyond doubt that cybercriminals' secrecy developed this malicious software through AI assistance in terms of the possibility of avoiding anti-virus detection and disrupting the victim's internal systems.⁸⁸ Moreover, such malwares are difficult they detect, upgrade themselves automatically and detect loopholes and vulnerability spots in the internal security systems. Therefore, upgrading the malicious software increases the risk of a personal data breach. The “soundly

⁸⁴ Hassanzadeh, Biddle, and Marsen, User Perception of Data Breaches.

⁸⁵ Jakrapong Kangwansophon, "Offenses of Fraud : Study of Telephone Scam Cases (Call Centers Gang)", *Research and Development Journal Bansomdejchaopraya Rajabhat University*, Vol.1, (May 12 2022): 280-290. ThaiJo, via ThaiJo, <http://www.thaijo.org>

⁸⁶ Philip, The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami.

⁸⁷ Ibid.

⁸⁸ Blauth, Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI.

distinctive” malicious software could take time until security weaknesses are discovered or suddenly attacked undetected, and the personal data obtained could be more silent than usual.

Additionally, AI is also implemented as a significant factor in cybersecurity.⁸⁹ The main factor in preventing cyber threats and cyberattacks in line with the upcoming AI role shall be defined as an unauthorised conveyancer the free (or premium feature by subscription) between the cybersecurity developer and the cybercriminal trying to invade the system and steal personal data unlawfully.⁹⁰ According to Personal Data Protection, the principle provides the Data Breach Notification Law.⁹¹ which enshrines the rudimentary principle of a “fundamental security system”. However, the data controller and data protection officer shall be responsible for taking control of the security system. When a personal data breach happens, this law shall be applicable to notify the data subject (personal data owner) and assess the damage that occurred to provide the tentative compensation to cure from the threat.⁹² To enhance the effectiveness of notification features, AI also holds an essential role in cybersecurity as the instructor and the improved analysis to upgrade an internal security system against cyberattacks.⁹³ However, from the nature of AI, the security system’s innate, and the imperfection of the program's error, it is observed that both cybercriminal and

⁸⁹ XiaoLing Wang, "Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime", *Journal of Physics: Conference Series*, (2020): 1–6. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/342263120_Criminal_Law_Protection_of_Cybersecurity_Considering_AI-based_Cybercrime

⁹⁰ Ajay Singh. Harsh Lohiya, "Study for Artificial Intelligence for Cybersecurity : Approach for Prevention of Cybercrime", *International Journal of Applied and Universal Research*, vol. 9, no. 6 (2022): 1–8. IJAUR, via IJAUR, www.ijaur.com

⁹¹ Zulhuda, *Cyber Law in Malaysia : Principal and Practices*.

⁹² Sandra Schmitz-Berndt, "Cybersecurity is Gaining Momentum – NIS 2.0 is on its Way", *European Data Protection Law Review*, vol. 7, no. 4 (2021): 580–585. EDPL, via EDPL, <https://edpl.lexxion.eu/article/EDPL/2021/4/14>

⁹³ Cristian-Vlad Oancea, "Artificial Intelligence Role in Cybersecurity Infrastructures", *International Journal of Information Security and Cybercrime* 4, vol. 1 (2015): 59–62. IJISC, via IJISC, <https://www.ijisc.com/articles/2015-01-08.pdf>

cybersecurity sectors emphasise the loophole of the error in the security system.⁹⁴ Cybercriminals may launch the invasion if loopholes exist because that is the perfect timing for unauthorised access, as mentioned above. Meanwhile, the cybersecurity team must fill and resolve those loopholes immediately to ensure safeguarding the system through normal functions. Therefore, this AI role shall be the Data Breach Risk Prediction as the strategist to examine the system's bugs, errors, and loopholes.⁹⁵ Circumstantially, it could be demonstrated that AI, in the middle, contributed to the “Tug-of-War” between cybercrime and cybersecurity, unavoidably by its functions and capability.

From the “Tug-of-War” to the role of “Breach Risk Prediction” in the cybersecurity perspective, the “security system loophole examination” became an essential factor in personal data breach operation and prevention.⁹⁶ Moreover, AI and the processing function are considered imperfect and cause some “error incidents”. These error circumstances are related to the accidental category of a personal data breach, as elaborated in the non-malicious section. In short, it is undeniable that AI may be used for both righteous and illegal purposes, such as personal data breaches. AI has significantly influenced the present and has addressed many legal issues, such as the subjectivity of AI in law, AI criminal liabilities, and the ethics of AI usage.⁹⁷ Thus, it is essential to address continued in-depth study in this subject to solve the current tug-of-war situation between cybersecurity and cybercrimes.

⁹⁴ Xichen Zhang, Data breach: analysis, countermeasures and challenges.

⁹⁵ Harsh Lohiya, Study for Artificial Intelligence for Cybersecurity: Approach for Prevention of Cybercrime.

⁹⁶ Blauth, Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI., 77114-77117.

⁹⁷ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024 PDPA practitioners are also aware of AI issues. Moreover, after Thailand declared the ethical direction of AI usage in 2022, the practitioners addressed the opinion that the next issue from PDPA is the AI that may be legalized on this upcoming technology.

4.4 CONCLUSION

An analysis of Thailand's legal framework uncovered both advantages and disadvantages that may influence the legal transplant process, particularly with adaption and contextualisation within Thailand's legal system. The primary challenge often faced while analysing this substantive legislation is the interplay between substantive and procedural laws under Thailand's legal framework. Such a paradox poses new challenges for legal practitioners in Thailand as they work to apply the five substantive enactments effectively in handling personal data breach scenarios. This research has identified areas to improve Thailand's legal implementation by investigating Thailand's administrative sanctions and specific procedural laws relating to personal data breaches, cybercrime, and cyber Threats. Thailand's legal framework has undergone significant changes, especially through complete enforcement in 2022 and 2023.⁹⁸ These paradigm shifts, aim to implement comprehensive measures and ensure institutional mechanisms are aligned with current legislation. The internal legal framework assessment is expected to provide valuable advice and solutions for managing uncontrollable Factors like "Technological advancement" and "Technical and Human errors" in the realm of personal data breaches, cybercrime, and cyber threats.

The comparison between Thailand's PDPA and EUGDPR in benchmarking analysis demonstrates that Thailand's legislation has successfully incorporated comprehensive Personal Data Protection measures, including prevention, suppression, detection, and recovery. This outcome is evident in various aspects, such as the appropriateness of the CIA framework, the Notifications Law, Complaint functionality for internal dispute resolution, and the multiple categories of sanctions. The analysis

⁹⁸ Annual Report 2023 : Thailand National Cyber Academy (TNCA).,130-135.

provides positive results for the internal legal practitioners, international reviewers, and commentators. Although discrepancies may exist between Thailand's rules and the EUGDPR, the core ideas remain intact.⁹⁹ Thailand's legislation adheres to the global information privacy standard exemplified by the EUGDPR. This benchmark indicates that Thailand's successful adoption of comprehensive legal measures suggests a future focus on Regional Cooperation in Personal Data Protection.

Last but not least, in agreement with Xichen Zhang and colleagues, technological advancement is the one uncontrollable factor that causes personal data breaches of cybercrime to remain in motion throughout cyberspace.¹⁰⁰ Artificial Intelligence (AI) proves that this technology has the role of enhancing the personal data breach effect of the operation to the next level, whether the complications and the damages to the victim contributed to many issues of this technology. The liability of malicious activity post such incidents by AI requires further in-depth studies, providing plausible solutions and management.¹⁰¹ Additionally, this upcoming technology began to affect Thailand as identity theft operations applied Deepfake technology negatively.¹⁰² Moreover, as described above, AI as the assistance in developing software and malicious software caused new upcoming threats as Thailand's legal practitioners focused and started a study intensely called Advance Persistent Threat (APT).¹⁰³ Thus, Thailand must remain on alert due to developing AI technology and comprehensively remain prepared for the proper arrangements and management of AI issues.¹⁰⁴

⁹⁹ Graham, Law Comment-From Thailand to Jersey – GDPR's Global Effect is Evident.

¹⁰⁰ Xichen Zhang, Data breach: Analysis, Countermeasures and Challenges.,433-437.

¹⁰¹ Phillip, The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami.

¹⁰² Jakrapong, "Offenses of Fraud : Study of Telephone Scam Cases (Call Centers Gang)".

¹⁰³ Annual Report 2023 : Thailand National Cyber Academy (TNCA).,131-135.

¹⁰⁴ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024.CSA practitioners addressed the AI malicious issues of this technology and developed the new malicious software, which detects cyber threat programs that failed to detect and suppress the threat,

Based on this discussion, this research continues to elaborate on the research findings, further recommendations and suggestions for upgrading Thailand's legal framework, and the conclusions in the next chapter, which is going to be the Conclusion of this dissertation.



called APT (Advance Persistent Threat). Moreover, an Identity theft operation launched the Deepfake features into impersonating Thailand's police as a manipulated victim into earning financial unlawfully. Thailand's CSA, CCA, and PDPA practitioners have started to become aware of the malicious use of AI and have studied this issue to be ready to encounter, handle, and suppress this upcoming technology.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

Chapters 1 to Chapter 4 have discussed the main personal data breach incident. To begin with, the background study is the situation of personal data breaches in Thailand at the peak level, which leads to the problem statements focusing on the new challenges in the application of the new legislation, specifically on PDPA and CSA 2019. Chapter 2 continuously highlighted the characteristics of personal data breaches to uphold the understanding of the details of operation processes, the study through the Islamic perspective. Afterwards, the study brought comprehensive legislation under Thailand's legal framework into elaborate and summarised overall legal measures implemented under personal data breach in Chapter 3. Lastly, Chapter 4 provides the internal legal analysis that lingers from the summarisation of legal measures into addressing the legal issues, whether from the interpretation and implementation of legislation based on the doctrinal and legal statutes. Moreover, the benchmark study between PDPA 2019 and EUGDPR 2016, as the global concur standards that perform the trustworthiness and reliability of Thailand's PDPA 2019, could be applied to this incident's accountability. Furthermore, the personal data breach has the development by itself that the study continues to provide in the subject of Artificial Intelligence (AI) usage. It is undeniable that the technologies still improve continuously and pose a significant challenge to the law in terms of both interpretation and implementation improvements.

This chapter shall bring these doctrinal research findings and outcomes into summarization to provide recommendations and suggestions. To conclude effectively, there is a need to highlight the data collection applications that have been utilized to produce the doctrinal research findings by the opinions of Thailand's legal practitioners.

These practitioners are responsible for the different enactments under Thailand's legal framework and they are:

1. General Dr. Pushpong Pongsiri, Chairman of the expert committee 2nd unit examination in the PDPC-compliant platform and the expert in social science under Thailand's NCSC, representative of Thailand's PDPA and Thailand's CSA practitioner,¹
2. Police Colonel Siriphon Kusunsinwut, Director of the Legal Department of PDPC Thailand, representative of PDPC Thailand²
3. Police Colonel Naughtakrid Phromchan, Director of Cyber Operation Office, representative of NCSA and Thai Cert unit,³
4. Dr. Udomtipok Praikaset, Chief Executive Officer and Mr. Sukris Koyakradej, Chief Data Privacy Consultant and Auditor of Digital Business Consultant Group (DBC group), representatives of Thailand's private sector responsible for Thailand's PDPA practices.⁴

Firstly, between 2018 to 2020, malicious computer activities heavily impacted Thai society as highlighted particularly by the AIS crisis, which is initially discussed in the background of the study. This has resulted in significant financial losses, cybersecurity challenges, and the need to compensate affected clients. The financial impact has involved hundreds of millions of Baht, with overall cyber incidents causing even higher economic losses.⁵ Furthermore, the complex nature of this crime involves intricate processes and tactics, including merging cybercrime with organized attacks,

¹ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya", Bangkok, 14 May 2024.

² Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024.

³ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024.

⁴ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024.

⁵ Ibid.

illicit computer schemes like ransomware for extortion, and the ongoing threat of identity theft and online fraud in Thailand.⁶ In response, Thai authorities have implemented legal measures to address these criminal activities.

The finding study on the nature of personal data breaches in Chapter Two reveals that they may be categorised into three categories:

1. External personal data breaches that involve a perpetrator acting as a hacker to disrupt the target system, a lesson learned from major crises like AIS and the 9-near incidents.
2. Internal personal data breaches known as data leak which are linked to "insider threat."⁷ This threat involves insiders' unauthorised purchase of personal data, which leads to cybercriminals using the information for activities like "identity theft" or scams. Since 2021, these have been challenges for Thailand's cybercrime suppression efforts.⁸ It is advisable to conduct further research on "data leak and insider threat" in Thailand.⁹
3. Non-malicious personal data breaches mainly occur due to errors, whether by the system or humans who are the instructors. This category does not involve the perpetrators in the two other categories mentioned above. Furthermore, this category could be addressed as the negligent personal data breach or accidental personal data breach incident.

⁶ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024..

⁷ Ibid.

⁸ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024.

⁹ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya," Bangkok, 14 May 2024.

5.1 Conclusion

The discussions in Chapter 2 continuously found that the Islamic perspective has a unique role in influencing the interpretation and implementation of the subject matter, which is explicitly different from Thailand's legal framework.¹⁰ The Buddhist perspective focuses on mind development through meditation.¹¹ Meanwhile, the Islamic perspective provides religious evidence for the privacy right with the grant of permission and the importance of secrecy.¹² Thus, the development of the legal framework from physical privacy to information privacy under the Islamic perspective still presents the legislation with improvement on the specific structure and the influence of the religious perspective. However, Thailand's legal framework has decided to be discretionary and selective. It launched the legal transplanted methodology,¹³ from constructing the legal system to developing information privacy in Thailand's legal framework. In short, the Chapter 2 study provides the nature and characteristics of the personal data breach. Continuously, the study also contributes to rudimentary rights of privacy and legal development in both theoretical and religious frameworks.

Chapter 3 summarises substantive legislation in Thailand's legal framework that governs the PDPA 2019 approach. These laws focus on the compliance obligations of

¹⁰ Abdurrahman Bello Onifade, et al, "Information Ethics: Islamic Perspectives on Privacy and Hacking", *Journal of Knowledge & Communication Management*, vol. 9, no. 1 (2019): 29–44. ResearchGate, via ResearchGate, <https://www.researchgate.net/publication/333510486>.

¹¹ Sneha Chawla, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments," (Unpublished Master's Independent Study Dissertation, Thammasart University, 2019).

¹² Marwan Albahar and Mohammed Thanoon, "Privacy Regulations in the Middle East: Challenges & Solutions", *International Transaction Journal of Engineering*, vol. 13, no. 5 (2022): 1–11. ResearchGate, via ReserachGate, https://www.researchgate.net/publication/360972272_Privacy_Regulations_in_the_Middle_East_Challenges_Solutions

¹³ Alan Watson, 1996. "Aspects of Reception of Law." *The American Journal of Comparative Law* 44 (2): 335. Heinonline, via Heinonline, <https://doi.org/10.2307/840712>.

the Data Controller and Data Processors and the Data Subject, who hold specific rights and responsibilities as outlined in the legislation. PDPA imposes various sanctions.¹⁴ Thailand's PDPC has jurisdiction over conducting discretionary examinations of compliance requirements and can impose administrative fines as the primary sanction under this Act.¹⁵ The Data Subject has the right to take legal action against the Data Controller and Data Processors for any unlawful actions, seeking compensation for actual damages and punitive measures as outlined in Sections 77-78 of PDPA.¹⁶ Legal professionals in Thailand respect the information privacy and cybersecurity compliance standards following the CIA principle¹⁷ as outlined in the PDPA and CSA enactments from 2022. Although the PDPA is undergoing a discretionary evaluation process, it is moving forward with the complaint function. According to the PDPA 2019, this will involve publishing orders related to data subject complaints from Thailand's Personal Data Protection Committee (PDPC).¹⁸

The table of summary in Chapter Three demonstrates two significant enactments, which are CSA and CCA. The second revision of CCA in 2017¹⁹ had primarily influenced the upcoming enforcement of CSA in 2019, which although they confronted each other, they supported the operation of the officer whether the CCA officer, Thai Cert, or CCIB following Thailand's cybersecurity policy and the strategies

¹⁴ Police Colonel Siriphon Kusonsinwut, "Interviewed by "Kornwat Kaewkulaya", Bangkok, 8 May 2024.

¹⁵ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya," Bangkok, 14 May 2024.

¹⁶ Theerachit Jitkarunawong, "Civil Liability under Data Protection Law: A Comparative Study of Thailand's Personal Data Protection Act And EU's General Data Protection Regulation (EUGDPR)", (Unpublished Master's. Independent Study Dissertation, Thammasart University, 2019).

¹⁷ Kanathip Thongveerawong, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, (Thailand: Nitithamlawbooks, 3rd edn., 2022).

¹⁸ Police Colonel Siriphon Kusonsinwut, "Interviewed by "Kornwat Kaewkulaya", Bangkok, 8 May 2024.

¹⁹ Sarawut Pitiyasak, *The Description of Thailand's Computer Crimes Act First and the Second Edition (2007 and 2017)*, (Thailand: Nitithamlawbooks, 3rd edn., 2021), 56-60.

of detection, suppression, and recovery.²⁰ Many proceedings have been successful because of this framework. In enforcement of the CSA, the legal practitioners had significant investment in cybersecurity and cyberthreat encounter operations whether the training of expertise, tools, and equipment. Significantly, the “forensic identity” investment caused the advancement of personnel operations.²¹

The table of amendments conclusively illustrates the central supporting role of legislation under the Tort Law principle under CCC. The fundamental criminal offence under the Penal Code is still continuously implemented as a confrontation of legal elements, each supporting the compensation principles. The practice through the Penal Code shall mainly address insider threats and cybercrime related to the financial societal context in Thailand, whether the officer's illegal action or the fraud and extortion offence.²² Respondents agreed and were satisfied with Thailand's current legal framework and measures that could solve the problem of legal interpretation, as mentioned in this dissertation. The intense application of “information privacy” is done through the influence of PDPA 2019 enforcement.²³

Regarding the effective implementation of Thailand's legal framework, this dissertation found that Thailand has been successful in comprehensively decreasing the frequency of cybercrime invasion. According to the annual report by NCSA, the statistics of cybercrime invasions, including personal data breaches, significantly reduced between 2022 and 2023.²⁴ Likewise, Statist” also reported that breaches of

²⁰ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024.

²¹ Ibid.

²² Ibid.

²³ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya," Bangkok, 14 May 2024

²⁴ Thailand National Cyber Security Agency, Annual Report 2022 by Thailand National Cyber Academy (TNCA), Thailand National Cyber Security Agency official website, 2023).https://ncsa.or.th/Ebook_%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A/files/basic-html/page1.html (Accessed 15 April 2024). 66-68.

online accounts in Thailand continuously decreased between 2022 to 2023.²⁵ Moreover, since 2022 and with adequate investment in cyber suppression, Thailand's officers could come into operation immediately and precisely detect and suppress a cyber threat. Because of the CSA framework, the NCSA and Thai Cert unit achieved the most satisfying achievement in Thailand, receiving the "CSO 30 ASEAN award" in 2023.²⁶ This proves that Thailand's legal measures are very effective whether the policies relate to strategies, prevention or suppression in the regional framework. As one of the leading cybersecurity countries,²⁷ the successes in Thailand are expanded from the achievement of the 9-near incident operations and JIB computer incident examination as elaborated in the milestone incident and PDPA sample case under this study.

The results of the benchmark analysis between Thailand's PDPA 2019 and the international standard EUGDPR 2018 in relation to the doctrinal aspect were satisfactory and agreed upon by Thailand's legal practitioners. The main principles of information privacy and data subject rights are transplanted comprehensively, and the multiple sanctions caused the Data Controller and Data Processors to adapt and enhance the system to uphold the regulations.²⁸ Thus, the positive comments made for the "*Explicit Personal Data Protection Regulation*"²⁹ as mentioned by the international doctrinal demonstrate the essential legal measure under PDPA.³⁰ It proves that PDPA has robust and conclusive legislation. The specific measures, such as the compliance duties of Data Controllers, the data breach notification law, and the complaint

²⁵ Statista Research Department, Number of breached online accounts in Thailand from 1st quarter 2020 to 2nd quarter 2023, <https://www.statista.com/statistics/1404553/thailand-number-of-account-breaches-exposed/> (Accessed 10 August 2024).

²⁶ Annual Report 2023 : Thailand National Cyber Academy (TNCA), 110-111.

²⁷ Ibid.

²⁸ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024..

²⁹ Graham Greenleaf and Arthit Suriyawongkul. "From Thailand to Jersey – GDPR's Global Effect is Evident." *Privacy Laws & Business International Report*, 2019, 2. Privacy Law and Business, via Privacy Law and Business, www.privacylaws.com

³⁰ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya", Bangkok, 14 May 2024.

proceedings under PDPC's supervision, regulate and address the implementation readiness. Furthermore, PDPA principles are confronted with other amendments and support each other in interpretation and implementation regarding personal data breach incidents and other cybercrimes.³¹

The progress of artificial intelligence (AI)³² aligns with previous studies, indicating ongoing advancements in technology and human error,³³ leading to improvements in addressing personal data breaches. However, challenges persist in determining the legitimacy of acquiring and handling personal data. In the ongoing battle between cybersecurity and cybercrime, it is anticipated that rapid adaptation will be necessary due to the increasing impact of AI technologies within the next five years. The "AI Act,"³⁴ implemented in the EU in February 2024, will soon become a focal point and impact Thailand's legal framework. Researchers interested in AI should take action and future research on AI should delve deeper into the subject.³⁵ Developing the "Guideline and Ethical Usage of AI"³⁶ in Thailand's legal framework is essential. The "legal transplanted" technique is anticipated to play a prominent role in future legislation in Thailand. AI's development is similar to the evolution of physical privacy

³¹ Police Colonel Naughtakrid Phromchan,"Interviewed by Kornwat Kaewkulaya", Bangkok,15 May 2024.

³² Philip Treleaven, et al., University College London, "The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami", *University College London*, (2023): 1–34. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/372399289_The_Future_of_Cybercrime_AI_and_Emerging_Technologies_Are_Creating_a_Cybercrime_Tsunami.

³³ Xichen Zhang, et al., "Data breach: Analysis, Countermeasures and Challenges", *Int. J. Information and Computer Security*, vol. 19 (2022): 402–442. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/365721658_Data_breach_analysis_countermeasures_and_challenges.

³⁴ European Parliament, European Union Artificial Intelligence Act.(EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (2024).<https://artificialintelligenceact.eu/ai-act-explorer/> (Accessed 20 April 2024)

³⁵ Police Colonel Naughtakrid Phromchan,"Interviewed by Kornwat Kaewkulaya", Bangkok,15 May 2024.

³⁶ Soraj Hongladarom, "The Thailand National AI Ethics Guideline: an Analysis", *Journal of Information, Communication and Ethics in Society*, vol. 19, no. 4 (2021): 480–491. ThaiJo, via ThaiJo, <http://www.thaijo.org>

into information privacy issues and the enactment of personal data protection regulations.³⁷ In the context of AI, the development duration has decreased from a decade to five years.

The outcomes of Thailand's legal framework assessments in Chapter Four of the study are combined with the opinions of Thailand's legal practitioners. These could be continued to be analysed and developed into research recommendations and suggestions. Moreover, these opinions can be used to propose further opinions and proposals for future studies and Thailand's legal revision regarding the Personal Data Protection Act and other legislation. The additional analysis from respondents to responses and encounters with cybercrime and personal data breach is discussed next.

Firstly, the respondents agreed with the ineffectiveness of Thailand's CCA legislation³⁸ even after the second revision, which is still not fully completed for implementation due to the recent cybercrime situation. Even though this legislation is based on ICT system offences, the proper way to sentence these cybercriminals should be better than the current version of CCA.³⁹ Specifically, in the encounter with "insider threats" and "internal personal data leak", the PDPA criminal liability is not covered. Also, the CCA framework applies only to illegal access and other specific fundamental criminal offences can also be used.⁴⁰ Therefore, it is suggested that Thailand's CCA still requires revision by legislators to enact precise and conclusive offences to confront the recent advances in cybercrime.⁴¹

³⁷ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024.

³⁸ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024.

³⁹ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya," Bangkok, 15 May 2024.

⁴⁰ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya", Bangkok, 14 May 2024.

⁴¹ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya," Bangkok, 15 May 2024.

Secondly, the interpretation and execution of subordinate laws in the PDPA framework by practitioners highlight that Thailand's legal system has advantages and disadvantages in how it is applied, which is achieved through contextualization. This process enhances the authority's system for assessing and ensuring the compliance of Data Controllers and Data Processors.⁴² It prioritizes effectiveness over solely relying on the primary PDPA. If the PDPA revision included all principles and secondary regulations, the process would be prolonged, potentially leading to delayed enforcement, as seen with the postponement of Thailand's PDPA in 2021.⁴³ Practitioners in CSA and CCA concurred with the statement regarding the accurate implementation of law when Thailand's legal framework is thoroughly used in court proceedings. Thailand's judicial and legal professionals must thoroughly understand how each law functions. If some principles are not implemented proficiently, it could result in misinterpretation of legislation and reduce the overall effectiveness of Thailand's legal framework on cybercrime, including issues related to personal data breaches.⁴⁴ Thailand's legal professionals should thoroughly understand law interpretation and application and exercise discretion while addressing cybercrime and cyberthreat events. Additionally, it is advisable to provide additional training for legal and technical staff to ensure they are adequately prepared for actual-world scenarios.⁴⁵

Thirdly, there are the intersecting matters between the notification law in CSA and the PDPA framework. CSA practitioners stressed that overlapping difficulties may arise. Both laws conclude that within the CSA framework, the obligation to comply with reporting cyberthreat incidents that pose a risk to critical information infrastructure

⁴² Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024.

⁴³ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024. .

⁴⁴ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024.

⁴⁵ Ibid.

(CII) sectors has led to the penalty for non-compliance.⁴⁶ PDPA has implemented mandatory compliance with "notification law," which is part of the CSA framework and allows for optional government intervention in specified cases.⁴⁷ Practitioners in the private sector are still investigating the overlapping issue, and the definition of Data Controller remains unresolved.⁴⁸ The interpretation of exemption principles in Section Four of Thailand's PDPA has been rather precise, impacting organizations that do not comply with the CSA and PDPA laws,⁴⁹ perhaps creating a loophole in law enforcement. Suppose the organization is exempted from CSA and PDPA regulations or needs a budget (as is familiar with medium enterprises) to comply with the rules and does not designate a Data Protection Officer (DPO) when incidents like personal data breaches happen. In that case, there is a risk of non-compliance with the "notification law" and reporting cyberthreat incidents.⁵⁰ Future studies should focus on the internal contradiction between Thailand's PDPA and CSA, especially CCA.⁵¹

Fourth, regarding the role of the fundamental code CCC and Penal Code, respondents agreed that some principles in the procedure law, such as class-action⁵² and Section 44/1 of the Criminal Procedure Code,⁵³ might significantly affect the law's implementation. However, PDPA practitioners emphasized that the authority conducted a responsible administrative fine only.⁵⁴ Still, the other liabilities shall take the response

⁴⁶ Ibid. The director's emphasis is the differences between CSA sections 57 and 58 and the additional benchmark with Thailand's PDPA 2019 section 37 (4). These two legislations are enforced on different subjects and issues.

⁴⁷ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya," Bangkok, 14 May 2024.

⁴⁸ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024.

⁴⁹ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024.

⁵⁰ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024.

⁵¹ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024.

⁵² Government Gazette, Thailand civil procedure code. (Volume 134) (Chapter 69 Gor) (Revised 2017).

⁵³ Government Gazette, Thailand's Criminal Procedure Code, (1934). (Volume 136) (Chapter 34 Gor) (Revised 2019)

⁵⁴ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024.

by a direct lawsuit to the court for the procedure.⁵⁵ Meanwhile, in most CCA cases, the prosecutor should conduct the case as the plaintiff.⁵⁶ Thus, it is believed that the parties should face the upcoming challenges from the personal data breach issue, whereby these highlighted principles shall support the procedure cases by providing the actual effectiveness of “appropriate compensation” and additional remedies regarding the personal data breach itself whose damages are large-scale.⁵⁷ Likewise, the administrative lawsuit regarding Thailand’s administrative law framework has the “appeal” function, which should be developed under this sanction category in further studies.⁵⁸

Lastly, regarding the CSA framework, the CSA’s practitioners addressed the legal issue as they operated in the actual incident and found that the problems with the CSA limitation are only related to government agencies and critical information infrastructure (CII) boundaries in the actual operation. The organization, which might potentially be interpreted under these terms, have many units but when they request emergency assistance from the cyberthreat incident, the Thai Cert could not provide full assistance due to this limitation.⁵⁹ Therefore, it is recommended that the legislator should consider expanding the definition regarding the CSA framework into covering another essential organization that might be concerned with the CII definition, whether the medium government agencies are excluded from this enactment or private CII

⁵⁵ General Pushpong Pongsiri, "Interviewed by Kornwat Kaewkulaya," Bangkok, 14 May 2024.

⁵⁶ Thailand’s Official Law Reports in Data Breach Case (Non-translation). <https://deka.supremecourt.or.th/>. (Accessed 15 April 2024)

⁵⁷ Police Colonel Siriphon Kusonsinwut, "Interviewed by Kornwat Kaewkulaya", Bangkok, 8 May 2024.

⁵⁸ Ibid.

⁵⁹ Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024. CSA practitioners are aware that the definition might not be covered comprehensively when applying this act in terms of implementation.

organizations that conduct the flagship enterprises and responsible for the CII structures.⁶⁰

To summarise, this study has examined the evolution of information privacy law in Thailand, with a particular focus on Thailand's Personal Data Protection Act (PDPA) 2019⁶¹ and its alignment with global standards such as the EU General Data Protection Regulation (GDPR).⁶² Chapter 2 reflected the theoretical underpinnings of personal data breach characteristics and the principles of privacy. The analysis of the influence of Buddhist and Islamic perspectives on legal interpretations. While Buddhist principles emphasize ethical self-regulation, Islamic teachings provide explicit religious guidelines reinforcing the significance of privacy protection. The findings indicate that Thailand has selectively integrated international privacy norms while adapting its legal framework to reflect its distinct socio-cultural and legal context. Furthermore, the reflection on personal data breach characteristics found that the main threats that Thailand is facing are external and internal threats.⁶³ Meanwhile, the non-malicious category rarely occurs and is not emphasised as mentioned above.

Chapter 3 provided an in-depth analysis of Thailand's key data protection and cybersecurity laws, including the PDPA 2019, CSA 2019, and CCA second revision 2017. The chapter outlined the compliance obligations imposed on Data Controllers and Processors under the PDPA, with oversight by the Personal Data Protection Committee (PDPC). However, regulatory inconsistencies persist, particularly in areas where the CSA and PDPA impose overlapping cyber threat reporting and notification principles

⁶⁰ Ibid.

⁶¹ Government Gazette, Thailand Personal Data Protection Act 2019.(Volume.136) (Chapter 69 Gor)

⁶² 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)
.https://gdpr-info.eu/

⁶³ Sneha, "The Concept of Privacy in Thailand and the European Union: A Comparative Study of Religious-Cultural Origins and Legal Developments".

to the authority's requirements. Additionally, this research has highlighted the CCA's limitations, particularly in addressing insider threats and unauthorised internal data breaches category.⁶⁴

A benchmark analysis in Chapter 4 assessed the PDPA in relation to the GDPR, identifying both strengths and areas requiring further refinement. While Thailand has effectively incorporated key GDPR principles such as data subject rights, compliance obligations, and breach notification requirements. The implementation challenges of Thailand's legal framework still remain. The discretionary nature of the PDPC's authority and the PDPA's restricted scope in addressing criminal liability present significant gaps in legal protection. Legal practitioners have also emphasised the necessity of further reforms, as reflected in the analysis of internal legislation. Thus, in terms of adapting the regulatory framework to address emerging threats such as artificial intelligence (AI) and increasingly sophisticated cybercrime tactics.⁶⁵

In conclusion, Thailand's legal measures have successfully addressed significant cyberthreats like personal data breaches.⁶⁶ The country's specific legislation offers prevention and suppression measures to combat these illegal activities. The doctrinal research demonstrates the success of the legal transplanted methodology within the field of comparative law.⁶⁷ The research highlights the ongoing importance of comparative law studies, particularly on the transplantation and contextualization of the EUGDPR into Thailand's legal framework, as discussed in the summary of Thailand's legal measures and benchmark study. Furthermore, this phenomenon has ceased to generate

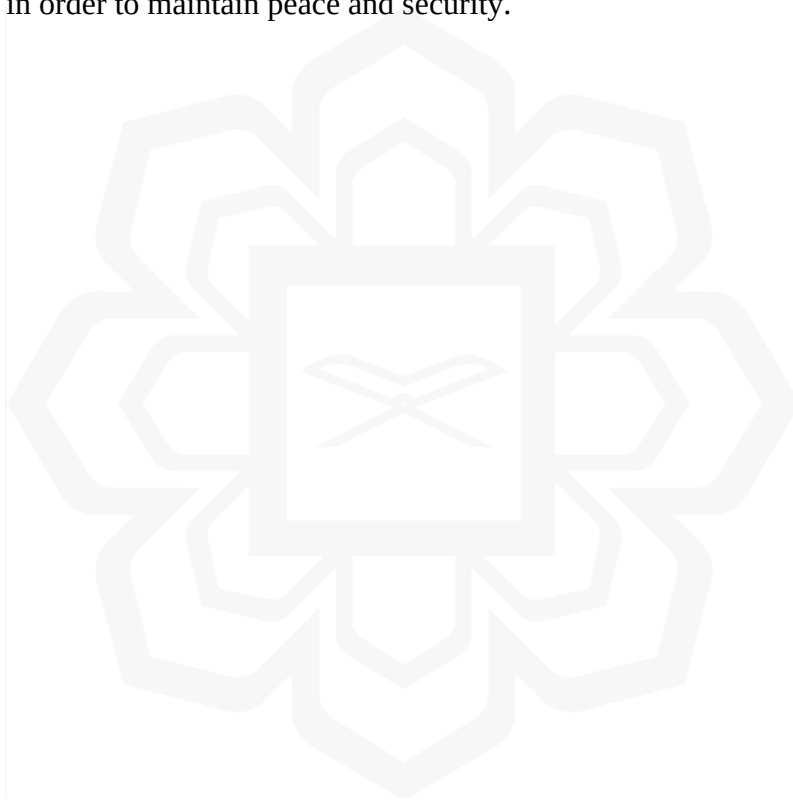
⁶⁴ Thailand's Official Law Reports in Data Breach Case (Non-translation).

⁶⁵ Philip Treleaven, et al., University College London, "The future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami", *University College London*, (2023): 1-34. ResearchGate, via ResearchGate, https://www.researchgate.net/publication/372399289_The_Future_of_Cybercrime_AI_and_Emerging_Technologies_Are_Creating_a_Cybercrime_Tsunami. 1-34.

⁶⁶ Annual Report 2023 : Thailand National Cyber Academy (TNCA).

⁶⁷ Alan, "Aspects of Reception of Law."

significant legislation and has succeeded in its execution,⁶⁸ as previously noted. Finally, the unpredictable element of technological progress in cyberspace⁶⁹, such as AI, is still present.⁷⁰ Thailand's sectors are prepared to enhance the legal framework to a higher standard, similar to the implementation of EUGDPR.⁷¹ All sectors in Thailand have been vigilant about this threat, implementing key legislation that has led to tangible achievements.⁷² Thailand is working on comprehensive measures to prepare for global challenges in society and cyberspace, with the support of ASEAN and international partners in order to maintain peace and security.



⁶⁸ Kanathip, *Specific Law Series: Thailand's Personal Data Protection Law Principle*, 518-520.

⁶⁹ Xichen Zhang, *Data Breach: Analysis, Countermeasures and Challenges*.

⁷⁰ Phillip, *The future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami*.

⁷¹ Sukris Koyakradej, "Interviewed by Kornwat Kaewkulaya", Bangkok, 11 May 2024.

⁷² Police Colonel Naughtakrid Phromchan, "Interviewed by Kornwat Kaewkulaya", Bangkok, 15 May 2024.

5.2 RECOMMENDATIONS AND SUGGESTIONS

- Further in-depth studies regarding the specific “Personal Data Leak” and “insider cyber threat” in Thailand’s society and circumstances. Moreover, Thailand’s legislators should address this issue of criminal liability regarding internal personnel committing Personal Data Leaks.
- Legislators should uphold the next revision in Thailand’s Computer Crimes Act to update criminal liabilities to confront and update the recent cybercrime circumstances.
- Further in-depth investigation of the contradiction or overlapping problem between Thailand’s PDPA, CSA, and CCA to enhance the effectiveness of law implementation regarding cybercrime and cyber threat incidents.
- Legislators should uphold the next revision in Thailand’s Cybersecurity Act to expand the definition of “Government Agencies” and “Critical Information Infrastructure” to cover the additional organizations that might be considered enacted under this enactment.
- Legal practitioners should uphold the implementation of “Class-Action” principles under Thailand’s civil procedure framework and section 44/1 under Thailand’s criminal procedure act to enhance the civil liabilities in Thailand’s PDPA framework and criminal liabilities in Thailand’s PDPA, CSA, and CCA frameworks.
- Legislators should address the revision regarding Thailand’s Procedures Law as the next revision in confrontation with the latest Thailand’s Court of Justice “Online purchasing” and “Cybercrime” Divisions.

- Further in-depth studies are required regarding the subjective nature of artificial intelligence, the potentiality of the AI act, and the legal transplantation under Thailand's legal framework.
- The further in-depth study of "Harmonization of Personal Data Protection Law in the ASEAN framework" should be addressed and contributed to the actual regional cooperation, including enhancing the role of the Privacy Digital framework masterplan of ASEAN in 2025 to approach in practicality as Thailand's legal practitioners ensure that Thailand's legal framework has the readiness into upholding the cooperation and play as the well-assistance role in this regional framework. Moreover, the possibility of adding significant legal dispute resolution functions as "arbitrations" in the regional framework is examined.
- Government Sectors shall intensely implement and enforce these current legislation to demonstrate the effectiveness of substantive legislation. Even though many challenges are faced by the unfamiliar as the new trend, this standard is essential to approach and manage not only the personal data breach event but holistically of PDPA, CSA, and CCA to maintain the tranquillity of society.
- All sectors should enhance the comprehensive training of technical and legal practitioners as the expertise to respond to cybercrime and cyber threat incidents sufficiently.
- All sectors should develop the Public and Private Partnership or "PPP" as the conclusive operation both in terms of the cybersecurity investment into the expansion of the standard security system to cover overall sectors and provide the policy to strengthening the prevention and approaching measures regarding the inclusive detection, suppression, and recovery strategies in cybercrime including

personal data breach as the actual partnership between the comprehensive assistance from Government and Private sectors.

- All sectors should spread as correctly understood and aware of “Personal Data Protection” principles and “Data Subject” rights to Thailand’s population holistically. This enhancement of precise knowledge upholds this importance, uses rights precisely, and prevents legislation misuse in any terms.



REFERENCES

- Act for the Establishment of and Procedure for Intellectual Property and International Trade Court, Volume 113 Section 55 Kor (1996). (Revised and Reprint 2015).
- Act on Establishment of Administrative Court and Administrative Court Procedure, Volume 116 Chapter 49 Gor (1999).
- Administrative Procedure Act, Volume 136 Chapter 69 Gor (1996) (Revised 2019).
- Abu Dawud, S. (2008). *Sunan Abi Dawud* (1st ed.). Darussalam Publishers.
- Albahar, M., & Thanoon, M. (2022). Privacy regulations in the Middle East: Challenges & Solutions. *International Transaction Journal of Engineering*, 13(5), 1–11. <https://doi.org/10.14456/ITJEMAST.2022.101>
- Al-Bukhari, M. I. (1997). *Sahih al-Bukhari* (1st ed.). Darussalam Publishers.
- Amarin TV. (2023a, April 8). ‘9 Near’ เป็นใคร? ทำไมยังจับไม่ได้? จำสิบโท จกข้อมูลคนไทย 55 ล้าน." (Who is 9-Near? Why could the authorities not arrest him? sergeant major second class who stole Thailand's population of 55 million. *Amarin TV*. <https://www.amarintv.com/spotlight/economy/detail/44003>
- Anwarullah. (1997). *The Criminal Law of Islam* (5th ed.). A.S Noordeen.
- Bangkokpost. (2020a, May 26). 3-Week Lapse for AIS Data Breach. *Bangkokpost*. <https://www.bangkokpost.com/business/1924112/3-week-lapse-for-ais-data-breach>.
- BBC Thai. (2023h, March 31). 9near: จับกุม จำสิบโท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว"9-Near surrender himself the hacker who claimed that earned 55 million record of Thailand's population data". *BBC Thai*. <https://www.bbc.com/thai/articles/cq5z3w5lwdx0>
- Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. *IEEE Access*, 10, 77110–77122. <https://doi.org/10.1109/ACCESS.2022.3191790>
- Bureau of Technology and Cyber Crime, Department of Special Investigation. (2021a). รายงานวิจัย พรบ กระทำผิดคอมพิวเตอร์ ศูนย์อาชญากรรม ไทย "The Research on the Effectiveness of Law Enforcement on Computer Crimes in the ASEAN Economic Community, a Case Study of Malaysia, the Republic of Singapore and the Republic of the Philippines". Department of Special Investigation Bureau website, (Unpublished).
<https://www.dsi.go.th/th/Detail/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A8%E0%B8%B6%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%A7%E0%B8%B4%E0%B8%88%E0%B8%B1%E0%B8%A2%E0%B9%80%E0%B8%9E%E0%B8%B4%E0%B9%88%E0%B8%A1%E0%B8%9B%E0%B8%A3%E0%B8%>

B0%E0%B8%AA%E0%B8%B4%E0%B8%97%E0%B8%98%E0%B8%B4%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9A%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%B1%E0%B8%9A%E0%B9%83%E0%B8%8A%E0%B9%89%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B9%80%E0%B8%81%E0%B8%B5%E0%B9%88%E0%B8%A2%E0%B8%A7%E0%B8%81%E0%B8%B1%E0%B8%9A%E0%B8%AD%E0%B8%B2%E0%B8%8A%E0%B8%8D%E0%B8%B2%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%84%E0%B8%AD%E0%B8%A1%E0%B8%9E%E0%B8%B4%E0%B8%A7%E0%B9%80%E0%B8%95%E0%B8%AD%E0%B8%A3%E0%B9%8C .

Chawin Aunpat. (2015a). Data breach Notification Law. *Thammasart Law Journal (Anniversary 60th years of Assoc. Prof. Suda Wisarupich)*, 277–287.

Chawla, S. (2019). *The concept of privacy in Thailand and the European Union: A comparative study of religious-cultural origins and legal developments*, [Unpublished Independent Study Dissertation Master's Thammasart University]. Thammasart University.

Civil and Commercial Code, Volume 141, Chapter 58 Gor (2024).

Civil Procedure Code, Volume 134 Chapter 69 Gor (Revised 2017).

Computer Crimes Act, Volume 124 Chapter 27 Gor (2007).

Computer Crimes Act Second Revision, Volume 134 Chapter 10 Gor (2017).

Council of Europe. (2014). Budapest Convention and Related Standards. Council of Europe. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

Consumer Protection Act BE2551, Volume 125 Chapter 38 Gor (2008).

Cybersecurity Act, Volume 136 Chapter 69 Gor (2019).

Eduardo Gelbstein, J. K. (n.d.). *Internet Governance Issues, Actors and Divides* (1st ed.). Diplofoundation and Global knowledge partnership.

Farvin, S., & Baharom, F. (2016). *Computer Crimes from Islamic Perspective and the Role of Secure Software Practice to Mitigate Them Monitoring Oriented Agile based Web Application Development Methodology for Small Software Firms in Jordan View Project the Development of Integrated Model and Intelligent Support System for Software Certification Process View Project*. [Conference presentation], PASAK 2016, Selangor. <https://www.researchgate.net/publication/303551027>

Fukuyama, F. (2000). *The great disruption: Human nature and the Reconstitution of Social Order*. Simon & Schuster.

Genral Pushpong Pongsiri. (2024, May 14). The summarisation and confirmation of the study in Thailand's legal measures in the event of personal data breach outcome representative: PDPC Thailand and NCSC Thailand [Official Interview].

- Graham Greenleaf. (2019a). Law Comment- from Thailand to Jersey – GDPR’s Global Effect is Evident. *Privacy Law and Business International Report*, 1–6.
- GDPR. (2018). *General Data Protection Regulation (GDPR)*. General Data Protection Regulation (GDPR). <https://gdpr-info.eu/>
- Hassanzadeh, Z., Biddle, R., & Marsen, S. (2021). User Perception of Data Breaches. *IEEE Transactions on Professional Communication*, 64(4), 374–389. <https://doi.org/10.1109/TPC.2021.3110545>
- Hopkins, M. (2019). Your Personal Information was Stolen? That’s an injury: Article III Standing in the Context of Data Breaches. *The University of the Pacific Law Review*, 50(3), 427–452.
- Information Act, Volume 114 Chapter 46 Gor (1997).
- Jeremy Barnett¹, P. T., Andrew Bud, D. B., Charles Kerrigan, E. F., Sally Sfeir-Tait, A. K., & University College London, M. S. (2023). The Future of Cybercrime AI and Emerging Technologies are Creating a Cybercrime Tsunami. *University College London*, 1–34.
- JIB Computer Co, Ltd. (2024a). The Official Announcement: The Maintenance Direction and Measures by JIB Computer Co, Ltd Facebook page. <https://www.facebook.com/PPTVHD36/photos/%E0%B8%9A%E0%B8%A3%E0%B8%B4%E0%B8%A9%E0%B8%B1%E0%B8%97-%E0%B9%80%E0%B8%88%E0%B9%84%E0%B8%AD%E0%B8%9A%E0%B8%B5-%E0%B8%84%E0%B8%AD%E0%B8%A1%E0%B8%9E%E0%B8%B4%E0%B8%A7%E0%B9%80%E0%B8%95%E0%B8%AD%E0%B8%A3%E0%B9%8C-%E0%B8%81%E0%B8%A3%E0%B8%B8%E0%B9%8A%E0%B8%9B-%E0%B8%88%E0%B8%B3%E0%B8%81%E0%B8%B1%E0%B8%94-%E0%B8%AB%E0%B8%A3%E0%B8%B7%E0%B8%AD-jib-%E0%B9%81%E0%B8%96%E0%B8%A5%E0%B8%87%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%93%E0%B9%8C%E0%B8%82%E0%B8%AD%E0%B9%82%E0%B8%97%E0%B8%A9%E0%B8%AB%E0%B8%A5%E0%B8%B1%E0%B8%87%E0%B9%80%E0%B8%81%E0%B8%B4%E0%B8%94%E0%B8%81%E0%B8%A3%E0%B8%93%E0%B8%B5%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%A5/972743194895388/>. (Accessed 24 August 2024)
- Jitkarunawong, T. (2019). *Civil liability under data protection law: A comparative study of Thailand’s personal data protection act and EU’s General data protection regulation (EUGDPR)* [Unpublished Master's Independent Study Dissertation Thammasart University]. Thammasart University.
- Kanathip Thongveerawong. (2022a). *Specific law series: Thailand’s Personal Data Protection Law Principle* (3rd ed.). Nitithamlawbooks.

Kangwansophon, J. (2022). Offenses of Fraud : Study of Telephone Scam Cases (Call Centers Gang). *Research and Development Journal Bansomdejchaopraya Rajabhat University*, 1, 280–290. <https://so06.tci-thaijo.org/index.php/rdibsru/issue/view/17452>

Kingdom of Saudi Arabia anti-cybercrime law, A/90 (2007).

Kingdom Saudi Arabia Personal Data Protection Law, No. M/19 (2021).

Lozonschi, C., Bahaya, I., & “Alexandru Ioan Cuza” Police Academy, Bucharest, Romania. (2023). *Artificial Intelligence and its Impact on Cybercrime*. [In Proceedings of the International Conference on Cybersecurity and Cybercrime]: Bucharest, Romania Vol. X (pp. 120–122).

Matichon Online. (2024, March 19). สธ.แจงแฮกเกอร์ประกาศขายข้อมูล เช็กแล้วไม่พบหลุดจากระบบสาธารณสุข."The Ministry of Health clarified that the hacker who posted the sell the patient's data is fake. The Ministry's confirmation that the personal data was not leaked from the Ministry of Health systems. *Matichon Online*. https://www.matichon.co.th/local/quality-life/news_4480163

Matichon Online. (2024, March 28). “JIB” Admitted that the Personal Data Breach had Happened. Thailand’s PDPC is Under Investigation for this Fact. *Matichon Online*. https://www.matichon.co.th/economy/news_4498411

Mohammad Hashim Kamali. (2008). *Right to life, Security, Privacy and Ownership in Islam*. Islamic text society.

Muhammad Akram Laldin. (2015). *Introduction to Shari 'ah and Islamic jurisprudence*. Cert Publications.

Narong Jaihar, N. sereerak, Supakeit supasaksuksakorn, Nichanun nunthasiriphon, & Prasit Piwawatanapanitch. (2022). *General Data Protection Regulation (Thailand's description version)* (4th ed.). T.press Ltd.

National News Bureau of Thailand. (2022, February 22). AIS to Implement Additional Security Measures after Cyber Attack. *National News Bureau of Thailand*. <https://thainews.prd.go.th/en/news/detail/TCATG220222153051899>

Neil Ford. (2023, December 5). List of Data Breaches and Cyber Attacks in 2023. *It Governance*. <https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023>

Nelson, S. D., Simek, J. W. (2019). The anatomy of a data breach. *Law Practice*, 1, 38–41. <https://heinonline.org/HOL/License>

NewsNation. (2023, September 17). Study: AI can Steal Passwords with 95% Accuracy. *NewsNation*. <https://www.newsnationnow.com/business/tech/study-ai-steal-passwords-95-percent-accuracy/>

- Oancea, C.-V. & Telekom Romania. (2015). Artificial Intelligence role in Cybersecurity Infrastructures. in *International Journal of Information Security and Cybercrime* (Vols. 4–4, Issue 1, pp. 59–62).
- Onifade, A. B., Akinwande, K. A., & Shehu, H. (2019). Information Ethics: Islamic Perspectives on Privacy and Hacking. *Journal of Knowledge & Communication Management*, 9(1), 29. <https://doi.org/10.5958/2277-7946.2019.00004.4>
- Patipon Wongsrikul. (2022, June 6). อาชญากรรมทางไซเบอร์ในประเทศไทย (Summarize Thailand's Cybercrimes Situations). Interrisk Asia (Thailand) Co., Ltd. <https://www.interriskthai.co.th/th/cybercrime-in-thailand/>
- PDPA Thailand. (2024). The First Decision from PDPC Thailand: an Administrative Fine in the Personal Data Breach Incident. <https://pdpathailand.com/pdpa-news/personal-data-protection-1st-fine-penalty/?srsltid=AfmBOoqndqP1hTaQmjRWccVe0zfk8jMPLnsmimvv-i7X6xnBgCgJGzf8>
- Penal Code, Volume 139 Chapter 28 Gor (2022).
- Personal Data Protection Act, Volume 136 Chapter 69 Gor (2019).
- Personal Data Protection Act Thailand. (2023, June 1). Summarizing: Thailand's personal data breach event 2018-2023. <https://www.facebook.com/photo/?fbid=649740717170892&set=a.642220761256221>
- Personal Data Protection Committee. (2024, January 12). ศูนย์เฝ้าระวังการละเมิดข้อมูลส่วนบุคคล – PDPC Eagle Eye "PDPC Established the Special Unit PDPC Eagle Eye for Monitor Personal Data Breach". *Official Personal Data Protection Committee Thailand*. <https://www.pdpc.or.th/2640/>
- Personal Data Protection Committee Thailand. (2024, February 15). ขยายผล ทลายเครือข่ายซื้อขายข้อมูลส่วนบุคคล ใน PDPA operation ep.7 (PDPA operation Ep.7: Thailand's Authorities Expanding the Operation to Suppress the Illegal Purchasing of Personal Data.) *Official Personal Data Protection Committee Thailand*. <https://www.pdpc.or.th/4174/>
- Personal Data Protection Committee Thailand. (2024, March 28). The Tentative Declaration in the “JIB” Personal Data Creach Case by Thailand's PDPC. *Thailand's PDPC official Facebook page*. https://www.facebook.com/story.php/?story_fbid=433047432569353&id=100075923001714&paipv=0&eav=AfbXcfn5685uYNgrNa_yXa3ziKLG55YxAlnKaS52ylnSlkv8UXs4QxgqEfFO6M8GWzM&_rdr
- Phaijit sawadisarn. (2014). *Computer usage in legal practice and laws related to computer* (5th ed.). chuanpim 50 ltd.
- Police Colonel Naughtakrid Phromchan. (2024, May 15). The summarisation and confirmation of the study in Thailand's legal measures in the event of personal data breach outcome representative: NCSA and Thai Cert [Official Interview].

- Police Colonel Siriphon Kusonsinwut. (2024, May 8). The summarisation and confirmation of the study in Thailand's legal measures in the event of personal data breach outcome representative: PDPA supervision authority PDPC Thailand. [Official Interview].
- Prapee Apichatsakol, W. M. (2020). The Analysis of the Implementation of the Computer-Related Crime Act B.E. 2550. *Rajapark Journal Vol.14 No.32 January-February 2020, 14*, 84–95.
- Quran. (2016). Al-Qur'an Al-Kareem - القرآن الكريم; Al-Quran - القرآن الكريم. <https://quran.com/>
- Rajan, A. V., Ravikumar, R., & Shaer, M. A. (2017). UAE Cybercrime Law and Cybercrimes — an Analysis. *IEEE Explore*, 1–6. <https://doi.org/10.1109/cybersecpods.2017.8074858>
- Rakngam, K. (2020). Legal Problem of the Determination of Offenses Concerning Computer Access according to Computer Crimes Act. *Journal of MCU Nakhondhat*, 7(9), 193–204.
- Richie, J. T. (n.d.). Tort Trial and Insurance Practice: Data Breach Class Actions (Vol. 32, Issue 5, 66–67).
- Rudolph Peters. (2005). *Crime and punishment in Islamic law, theory and practice from the sixteenth to the twenty-first century*. Cambridge University Press.
- Sarawut Pitiyasak. (2021). *The Description of Thailand's Computer Crimes Act First and the Second Edition (2007 and 2017)* (3rd ed.). Nitithamlawbooks.
- Santoso, T. (2011). Implementation of Islamic Criminal Law in Indonesia: Ta Zir Punishment as a Solution? *IIUM Law Journal*, 19, 123–148.
- Sawaeng Boonchalermwipas, & Atiruj Tunboonchareorn. (2022). *The Thai legal history* (20th ed.). Winyuchon.
- Sawatree Suksri. (2020b). *The law and regulations about computer crimes and cybercrimes* (2nd ed.). Faculty of Law Thammasart University.
- Schmitz-Berndt, S. (2021). Cybersecurity is Gaining Momentum – NIS 2.0 is on its Way. *European Data Protection Law Review*, 7(4), 580–585. <https://doi.org/10.21552/edpl/2021/4/14>
- Singh, A., & Lohiya, H. (2022). Study of Artificial Intelligence for Cybersecurity: Approach for Prevention of Cybercrime. *International Journal of Applied and Universal Research*, IX(VI), 1–2. <https://www.ijaur.com>
- Soraj Hongladarom. (2021). The Thailand National AI Ethics Guideline: an Analysis. *Journal of Information, Communication and Ethics in Society*, 19(4), 480–491. <https://doi.org/10.1108/JICES-01-2021-0005>

- Statista Research Department,. (2023, August 10). Number of Breached Online Accounts in Thailand from 1st quarter 2020 to 2nd quarter 2023. *Statista*. <https://www.statista.com/statistics/1404553/thailand-number-of-account-breaches-exposed/>
- Sukris Koyakradej, Udomtipok praikaset. (2024, May 11). The summarisation and confirmation of the study in Thailand's Legal Measures in the event of personal data breach outcome Representative: Private sector DBC group [Official Interview].
- Suneti Kongthep. (2015). (n.d.). *Demonstrations of Thailand's Computer Crimes Act*. Krungsiam Publishing.
- Sunnah.com. (2019). *Sunnah.com - sayings and teachings of Prophet Muhammad (صلى الله عليه و سلم)*. Sunnah.com. <https://sunnah.com/>
- Thailand Consumer Council. (2024i, February 9). เร่ง ‘กรมกิจการผู้สูงอายุ’ แจ้งเตือนผู้สูงวัย หลังข้อมูลเกือบ 20 ล้านชุดโดนแฮ็ก "MDES strengthen department of older persons into notified and clarification to the elderly injured person regarding the recorded of 20 million personal data got hacked. *Thailand consumer council*. https://www.tcc.or.th/09022567_elder-information-leak_news/
- Thailand National Cyber Security Agency. (2022). The summarisation operation report 2021-2022 by Thailand National Cyber Academy (1–39) [The summarisation operation report]. Thailand National Cyber Security Agency.
- Thailand National Cyber Security Agency. (2023). Annual report 2022 by Thailand National Cyber Academy (TNCA) (1–156) [Annual report].
- Thailand National Cyber Security Agency. (2024, January). Annual Report 2023: Thailand National Cyber Academy (TNCA). *Thailand National Cyber Security Agency official website*. https://ncsa.or.th/Ebook_%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A/%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%88%E0%B8%B3%E0%B8%9B%E0%B8%B5%20%E0%B8%AA%E0%B8%81%E0%B8%A1%E0%B8%8A%202566.html
- Thailand Constitutional, Volume 134, Chapter 40 Gor (2017).
- Thailand's Court of Justice. (2022f, February 1). ดีเคย์! เปิดบริการแล้ว “แผนกคดีซื้อขายออนไลน์ในศาลแพ่ง” มุ่งคุ้มครองผู้บริโภค จากพิษซื้อขายออนไลน์ สินค้าไม่ตรงปก โฆษกศาลยุติธรรม ย้ำฟ้องออนไลน์ได้ 24 ชม. ไม่จำกัดวงเงินมากนัก เน้นเก็บหลักฐานสั่งชื้อจ่ายเงินสงศาล พร้อมติดตามความคืบหน้าคดีได้ใน 12 ชม.กรุงไทยร่วมพัฒนาช่องทางยื่นฟ้องผ่าน e-Filing ตามสโลแกน “ความยุติธรรมที่เข้าถึงง่าย.” "D-Day Court of Justice declared the opening of e-commerce special division operations under civil court division. Court of justice spokesman emphasised that the 24-hour filling also available with the slogan [the justice is easily accessible]". *Thailand's Court of Justice*. <https://www.coj.go.th/th/content/category/detail/id/8/iid/278977>

Thailand's Court of Justice. (2024, April 3). ประธานศาลฎีกา เปิดแผนคดีอาชญากรรมทางเทคโนโลยีในศาลอาญาแผนกคดีฟอกเงิน ฯ ในศาลแพ่ง จัดผู้เชี่ยวชาญประจำแผนก เริ่มทำการ 2 เม.ย. พร้อมจัดการคดีเฉพาะทาง สร้างความเที่ยงธรรมรวดเร็ว (Thailand's Court of Justice officially established the cybercrime division). *Thailand's Court of Justice*. <https://www.coj.go.th/th/content/category/detail/id/8/iid/407872>

Thailand's Criminal Procedure Code (1934). Volume 136, Chapter 34 Gor, Revised and Reprint 2019.

Thailand's Official Law Reports in Data Breach Case (Non-translation). (2023, November 10). Supreme Court (Court of Justice of Thailand). Retrieved April 15, 2024, from <http://www.supremedekacourt.co.th>

Thailand's PDPA Pro. (2021, May 14). เลื่อน !! PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล เริ่มใช้ปี 65 พร้อมแนวทางการรับมือของภาคธุรกิจ (Thailand's legislature decided to postpone Thailand's Personal Data Protection Act 2019 to 2022 due to reforming the private sector systems). *Thailand's PDPA Pro*. <https://pdpa.pro/blogs/postpone-of-pdpa-and-guidelines>

Thaipbs world. (2022, October 29). Hai Officials were Arrested for Selling the Personal Information of over 1,000 People to a Call Centre Gang. *Thaipbs world*. <https://www.thaipbsworld.com/3-thai-officials-arrested-for-selling-personal-information-of-over-1000-people-to-call-centre-gang/>

Thaipbs world. (2023, April 12). มอบตัวแล้ว “จาสิบโท” แสกเกอร์ “9Near.” "9-Near already surrender himself to the authority". *Thaipbs world*. <https://www.thaipbs.or.th/news/content/326573>

Thairath Online. (2022, February 4). Another Day, Another Data Breach: Thai Students' Data Hacked, Sold on Dark Web. *Thairath Online*. <https://www.thairath.co.th/news/society/2305233>

The AI Act Explorer | EU Artificial Intelligence Act. (n.d.). <https://artificialintelligenceact.eu/ai-act-explorer>

The Office of the Personal Data Protection Committee (PDPC). (2024l). Annual Report 2023 by Thailand Personal Data Protection Committee (PDPC) (pp. 1–88) [Annual report]. The Office of the Personal Data Protection Committee (PDPC).

The subordinate legislation consists of notification of committees, emergency royal enactments, and internal regulations under Thailand's Ministry of Digital Economy and Society. (MDES) Last update March 2024 (2024). <https://www.mdes.go.th/law>

Theft via the Internet and the Application of Hadd. (2023, November 15). Islamonline. Retrieved March 11, 2024, from <https://fiqh.islamonline.net/en/theft-via-the-internet-and-the-application-of-hadd/>

Unauthorized Access Proceedings (United Kingdom).

United Nations. (1948, December 10). Universal Declaration of Human Rights. United Nations; United Nations. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

Vice presiding Judge of Udon Thani Provincial Court, T. B. (2023, January). The Principle of Piercing the Corporate Veil with Consumer Protection [Official Court of Justice articles]. *Official Court of Justice articles*. https://library.coj.go.th/pdf-view.html?fid=51341&table=files_biblio

Watson, A. (1996). Aspects of Reception of Law. *The American Journal of Comparative Law*, 44(2), 335.

XiaoLing Wang. (2020). Criminal Law Protection of Cybersecurity Considering AI-Based Cybercrime. *Journal of Physics: Conference Series*, 1–6. <https://doi.org/10.1088/1742-6596/1533/3/032014>

Yrd. Doç. Dr. Recep ÇĞĞDEM. (2004). Concept of Ta'zir (Discretionary Punishment) in Theory and in Practice. *K Üniversitesi Hukuk Fakültesi Dergisi*, 167–185.

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., Canadian institute for cybersecurity (CIC), Faculty of Computer Science, & University of New Brunswick (UNB). (2022). Data Breach: Analysis, Countermeasures and Challenges. In the Canadian Institute for Cybersecurity (CIC) & University of New Brunswick (UNB), *Int. J. Information And Computer Security* (Vol. 19, Issue Nos. 3/4, pp. 402–442).

Zulhuda, S., & Mohamed, S. (2015). The Shari'ah Approach to Criminalise Identity Theft. In *Article in Pertanika Journal of Social Science and Humanities* (pp. 169–182). Universiti Putra Malaysia Press. <https://www.researchgate.net/publication/316524215>

Zulhuda, S., & Ridoan K. (2024). *Cyber law in Malaysia : principal and practices*. Sweet and Maxwell.

Zulhuda, S.. (2010a). *Information security in Malaysia: A legal framework for the protection of information assets*. [PhD Thesis International Islamic University Malaysia.]. International Islamic University Malaysia.

Zulhuda, S. (2010b). Information Security in the Islamic Perspective: The Principles and Practices. [Conference paper] *International Conference on Information and Communication Technology*. Jakarta, Indonesia. <https://doi.org/10.1109/ict4m.2010.5971936>

ธนนท์ทัต สุทธิยานิติกักดิ์ (Thanontus Suthiyanitipakdi). (2016). *Computer Crime: A case study of the prevention of unauthorised access to the computer systems* [Research Proposal Master's Dissertation Mahidol University]. Mahidol University.

APPENDIX I: THE SUMMARY REPORT OF THE INTERVIEW WITH VARIOUS RESOURCES FROM THAILAND SUBJECT MATTER EXPERTS



1. Police Colonel Siriphon Kusonsinwut, Representative of PDPC Thailand (8/5/2024) [Director of Legal Department of PDPC Thailand]

- From the nine near crisis and JIB incident, the responsible authority found some suggestions that the scope of PDPA criminal liability with the “Data Controller and Data Processor” is subjective, which from the fact the offender is the “Ex-Data Controller Employee” and the offender is not the actual data controller. This fact is a concern as the lacuna of PDPA criminal liability application imprecisely affects law implementation. Thus, this problem in law interpretation and Implementation should be addressed to develop and clarify the precise liability for this involving cybercrime (illegitimate data purchasing).
- It is agreed that the CCA framework seems slightly ineffective in implementing Personal Data Breach crimes due to the “Illegal Access” being limited to “Computer- Related” crime only, not in the total cybercrime, and the PDPA framework still consists of the boundaries in the compliance of the PDP regulations. The essential review and revision in the overall cybercrime, whether CCA PDPA CSA, still need to be addressed in the following law revision.

- The correct understanding of the rights of complaint function by the “Data Subject” still faced the misinterpretation problem. The actual case complaints statistics found many cases that exceeded the limit authority from PDPC Thailand. Indeed, the Administrative Fine and sanction are under the supervision of PDPC Thailand, but Civil and Criminal Liability are under the Court's Jurisdiction to prosecute. Therefore, announcing the correct understanding and enhancing awareness of PDP regulation among Thailand's population is essential.
- It is agreed with the study's outcome that the benchmarking between Thailand's PDPA and EUGDPR is satisfied. However, the in-depth interpretation of the standard of CIA principles and subordinate legislation still requires discretionary implementation with precise cases to provide fairness, integrity, and legitimacy for the parties and stakeholders.
- It is agreed that the upcoming AI is truly challenging Thailand's Legal framework due to the “Technological advancement” being faster than transactions from the information era into the PDP era. Thailand did not overlook this phenomenon and has prepared the appropriate legal framework to adapt for further enactment soon in AI, whether the general principles or malicious activities from AI. It is determined that the phenomenon of EUGDPR in Thailand's PDPA and AI Act in Thailand legislation might use a similar methodology.
- It is agreed that Regional cooperation, especially ASEAN in PDP, is necessary as the prototype of EDPS (European Data Protection Supervisor) that Thailand's Legal Framework could not adopted due to the responsibility exceeded. Therefore, it is recommended that this in-depth study of “Harmonisation of Personal Data Protection Law in the ASEAN framework” should be addressed and contributed to the actual regional cooperation, including enhancing the role of the Privacy Digital framework masterplan of ASEAN in 2025 to approach in practicality as Thailand's Legal practitioners ensure that Thailand's Legal Framework has the readiness into upholding the cooperation and play as the well-assistance role in this regional framework.



2.Mr. Sukris Koyakradej, Representative of the Private sector (Digital Business Consultant Group “DBC” group) [11/5/2024] [Chief PDPA Consultant and Auditor]

- It is agreed with the result of doctrine analysis that the Personal Data Breach has complicated characteristics, whether the processing of invasion or the multiple cybercrime approach. Moreover, this malicious activity connects with many personal data misses, which should addressed as “counterfoil” or cybercrime.
- With the summarisation of Thailand’s legal measures in the event of a personal data breach, he addressed that the PDPA, CCA, and CSA frameworks have been categorized according to the different purposes of each enactment. Firstly, the PDPA structure plays the role of the arrangements as the “Pre-breach incident,” which illustrates the compliance with regulations. This was followed by the CSA, which was the actual management role when the “Personal Data Breach Threats” occurred in the subjective of “Government Agencies” and approached with the “Notification, Detection, encountering, and recovering.” The Computer-related crime under CCA shall be applied to the original offender who committed a personal data breach. Therefore, the current legal framework with

the explicit structure of legal measures seems to carry out the comprehensive status and readiness for implementation.

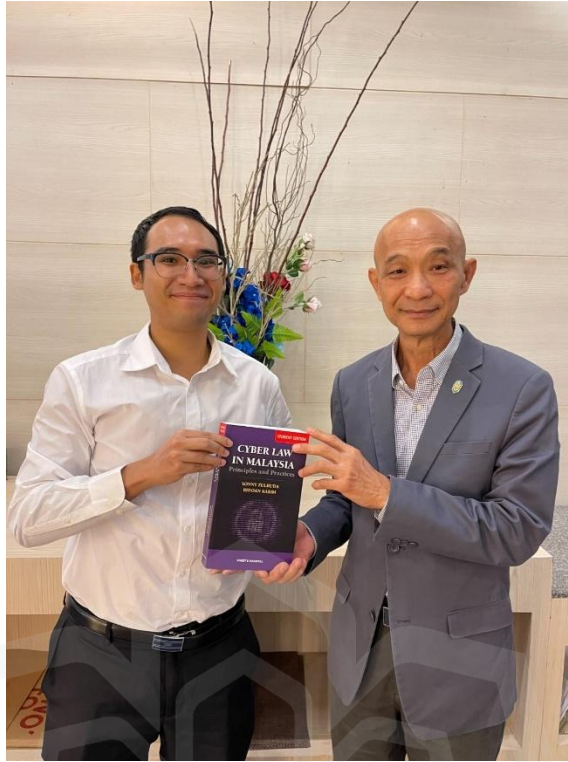
- From the outcome of the doctrinal study, it is agreed that the “Overlapping” situation might occur even if PDPA and CSA have explicit and separate enactments. The potential problem might arise when “the SME organization” has an insufficient budget to invest in the cybersecurity system and appoint DPO (data protection officers). This problem should be carefully followed and addressed with precise handling. [especially the minor healthcare and service based of organizations like tourism, massage, and entertainment.] Meanwhile, the problem of subordinate legislation interpretation as the legal practitioner examined this “contextualization” effect has systematically been linked to Thailand’s legal framework. If the total principles of Personal Data Protection are applied under the ACT or Royal Decree, the edition and law revision might delay the time into discretionary review. Therefore, this system of subordinate legislation shall belong to the supervision authorities and be more effective under Thailand’s legal system's context of interpretation and implementation.
- The consideration point in terms of the “Legal transplanted” phenomenon is addressed that Thailand’s PDPA has been transplanted because of a lack of background experience with the PDP implementation, which EUGDPR established from many lessons learned since the upholding issues by Prof. Shoshana Zuboff (Thailand’s Legal Framework effected from the “Cross-border data transfer principles”). Therefore, the essential expertise training and intense implementation of Thailand’s PDPA should be upheld, whether in Private or Government Sectors. From the examination and as a legal practitioner, I found that although this methodology is effective, some interpretation issues might occur, especially the definition of “Data Controller” and the exemption principle under section 4 of PDPA. Therefore, this should be a “discretionary” interpretation and implementation. Lastly, as the outcome of contextualization, it should uphold the regional issue to contribute to regional cooperation. The EDPS, in the context of ASEAN, might face difficulties due to the different partnerships between the EU and ASEAN. Nevertheless, Regional collaboration is the “Privacy Framework 2025”, and this issue should be addressed and started with the leading role in the region as Thailand, Malaysia, Singapore, and

Indonesia to establish and lead the way in standardized Personal Data Protection Principles.

- It is agreed that “technological advancement” is the uncontrollable factor; also, the original “Cyber Law” is the “Law of Horse” by itself. Thus, it is suggested that the government sector implement this legislation carefully, specifically regarding the limited rights and freedoms of Thailand’s population. Likewise, the upcoming AI Act is similar to the EUGDPR phenomenon as it addresses problematic issues and the direction of draft and enforcement. This act prevented the expected risk, threats, and unethical or malicious activities using AI. Thailand will likely bring this enactment to be drafted and enforced in a few years. [“Data is the new oil, AI is the new electricity”]
- Finally, the recommendations and suggestions can be divided into three categories: 1. Government Sectors shall intensely implement and enforce this current legislation to demonstrate the effectiveness of substantive legislation. Even though many challenges are faced by the unfamiliar as the new trend, this standard is essential to approach and manage not only the Personal Data Breach event but holistically of PDPA, CSA, and CCA to maintain the tranquility of society. 2. Under the Private sector, which conducted the role of “Data Controller and Data Processors,” the critical problem is known as the “Investment to comply with the standard of Cybersecurity,” including the “Recovery of the cybersecurity system after facing cyber-attack circumstances,” high. It might require some assistance from the government sector to conduct the additional policy, including some assistance to spread the “appropriate security standard” comprehensively. Moreover, the expertise regarding current legal measures is still in high demand. It is suggested that the government sector continue to produce and train the quality of “expert” professionals to be sufficient in the country. 3. Thailand’s Population still lacks awareness of “Data Subject Rights,” which could be determined in the “give the personal data more than required to Data controller” and “use the complaint function to supervision authority (PDPC Thailand) incorrectly” as the highlighted addressed issue in “Thailand digital economy forum” that the “Safety Awareness” is the one angle of the achievement but in the practical still ineffective into understanding the “Data Subject Rights” appropriately. Therefore, it is suggested that private and

government sectors continue to spread awareness, importance, and correct understanding of “Data Subject Rights” to Thailand’s population.





3.General Pushpong Pongsiri, Representative of NCSC and PDPC Thailand [expert in cybersecurity and the chairman of PDPC investigation committee 2nd unit] (14/5/2024)

- The situation of Cybercrime in Thailand, specifically the “Personal Data Breach,” has essentially addressed issues distinctive of “Data Breach” in Thailand, mostly “Internal Personal Data Breach,” also known as “Insider threats,” which is illustrated through the internal officer bringing personal data into the organization’s storage and sole illegitimately whether directly or indirectly to the cybercriminals or dark web platforms. Therefore, this issue should be significantly addressed in further in-depth studies. Moreover, “Thailand’s Insider threat” or “Data Leaked” occurred in both the government and private sectors and continues to happen until recently.
- With the current legislation measures, it is agreed that Thailand carried the comprehensive measures from the various Acts whether CCA, PDPA, and CSA by each enactment have the specific purpose of implementing whether compliance duty, preventive measures, detection, suppression, recovery, and execution with these enactments. From the doctrine study outcome, the subordinate legislation interpretation and implementation are problematic because each legislative entity explicitly has different purposes and roles in the

implementation itself. However, in the practical situation, some issues still need to be wholly inclusive for the combination of operations due to the legislation divided into many units, whether CCIB, Thai Cert, PDPA Eagle Eye, etc. Therefore, it is recommended that the authorities enhance and uphold the effective combination of operations with the current authorities, which is a significant achievement in the 9 Near case.

- It is agreed with the statement of the potential for development under the Regional cooperation, which should address another fruitful coordination in terms of the “arbitration” should develop and enhance the “Harmonization” of the Personal Data Protection legal framework in the ASEAN framework to ensure that when the “International Jurisdiction” dispute shall be resolved with the fairness of the proceedings and judicial authority shall evade the inflation of the disagreement that suits to the court proceedings.
- It is agreed that Thailand’s recent legal Framework significantly affects handling the “Personal Data Breach” and “overall Cybercrime” frequency statistics. 2022-2023 could highlighted as the significant year that after the full enforcement of PDPA, the legislators and authorities such as NCSC, NCRC, and PDPC announced the “subordinate legislation,” which not only the details of compliance duty but also the power of the officer under the authority supervision which as the multiple authorities unit also importantly advancement of CCIB and Thai Cert in the equipment and tools to handle with the “Forensic Identity” challenges. This could be illustrated through the combination of operations and the significant decrease in the statistics in the NCSA Annual Report from 2022 to 2023.
- It is recommended that every sector widely understand the Personal Data Protection principle for Thailand’s overall population because, according to the statistics of the PDPC-compliant platform, many complaints from the “Data Subject” are still misusing this function. Moreover, some complaints use the legislation as a “tool,” which might lead to unethical complaints and unnecessary suits against PDPC Thailand.



4. Police Colonel Naughtakrid Promchan, Director of Cyber Operation Office [representative of NCSA and Thai Cert](15/5/2024)

- Firstly, in the characteristic of the Personal Data Breach part, it is essentially agreed with the Government Sector Legal Opinion (Pol. Col. Siriphon and Gen. Puchapong) about Thailand's Cybercrime situation, specifically in Personal Data Breach which could be divided into two categories which are 1. The external personal data breach could be demonstrated in terms of the "Invasion of hackers" as the "9 Near" crisis example, and 2. The "Internal Personal Data Breach," also known as "the Insider Threat," primarily the actual

case, shall be considered under the “Insider Threat” or as known as the “Data Leaked” as the offender shall have understood the internal target system and sophisticated skill of technology which the intention of the perpetrator mainly is the “Illegitimate financial gain” whether the perpetrator shall “Illicit” disclose these personal data as the illegitimate purchasing of personal data with the cybercriminal or sold in dark web platforms. It is recommended that the issue of “the Insider Threat” in Thailand’s Cybercrime situation be addressed and developed as further in-depth studies.

- Secondly, it is agreed that Thailand’s current legal Measures carried out a comprehensive role since the PDPA conducted the compliance and the subjective “Data Controller Data Processor and Data Subject” CSA conducted the approaching strategy of the detection and suppression of “Cyberthreat” which caused to the CII (the critical infrastructure), the CCA shall arrange and pursue the offender who committed the “Computer-Related” crime and the primary supportive role from the CCC and Penal code which support the general Tort Law and the general criminal offence in which involved with the crime with the actual property such as fraud and extortion which implied with the online fraud as the scammers and ransomware. These five legislations also have specific characteristics and are conducted for a particular purpose. Also, this enactment shall fill the loopholes between them when some components might not be applied when the incident occurs. However, it is agreed with the legal framework assessment that the “subordinate legislation” carried out the overall details of principles, which the legal practitioner shall discretionarily examine. It might cause a problem when these laws are under judicial procedure. Therefore, the legal practitioner must understand these practices well to interpret and implement the law effectively. Moreover, the “Forensic Identity” is the true challenge of law implementation as legal practitioners found that many organizations and sectors require the essential understanding to implement and apply the facts. Furthermore, relying only on the specific division might not be conclusively effective in handling overall cybercrime circumstances, including the personal data breach incident. Thus, it is recommended that understanding the PDPA, CSA, and CCA principles be spread to the overall sectors and Thailand’s population is significant.

- Thirdly, regarding the overlapping issue in the “Notifications Law” between PDPA 37 (4) and CSA 57 and 58, indeed, the regulation slightly uses different terms as PDPA conducted the compliance duty as “Notify and informed” to the supervision authority. Still, the CSA framework compliance duty related to the “Administrative fine sanction” is the “CII cyber threat report,” not the notifications law under section 57 of CSA. In contrast, the notification duty from the government agencies is considered “optional,” which, if the organization is informed, shall not be subject to the sanction in CSA. Therefore, the government sectors shall examine these issues and voluntarily comply with the PDPA and CSA. However, in the CSA framework, the “evaluation of level in the cyber threat” and the response through the extreme level of cyber threat might occur. Thus, legal practitioners under the CSA framework should continue to examine the overlapping problem and solve it to find the most effective approach to this enactment's “Detection, suppression, recovery” measures.
- Fourth, it is agreed that Thailand’s current legal measures under five legislations successfully suppress the overall cybercrime situation in Thailand, especially in 2022-2023. Moreover, the CSA, CCIB, and CCA officers have significantly increased the capacity and capability of the equipment and personnel to handle these circumstances. Furthermore, CSA has carried out prevention measures and approaches to investigation using the detection strategy under the “Cybersecurity Policy.” Therefore, this policy significantly strengthens the officer's operation.
- Fifth, Regarding AI issues in the situation of “Tug-of-war” between the usage of this AI in cybersecurity and cybercrime operations, it depends on the user. Technological advancements have contributed not only to another complicated personal data breach process. Still, it contributed to the next level of threat as known as “Advance Persistent Threat or “APT,” which came in terms of “Float ware,” which developed from “Adware” with the parallel significant growth by the assistance of AI the practitioners whether the technological sectors or legal sectors should be addressed and continue to study the upcoming of technological advancement into precise handling and responding. It is believed that the AI Act shall come to control and manage AI's malicious and unethical usage, which fills the loophole that CCA and PDPA couldn't apply. However, like humans,

AI has recently been incomplete, which still causes “errors.” Therefore, the usage of AI still requires discretionary instruction and usage, as well as an examination of the correct outcome of their products.

- Lastly, the recommendations and suggestions Firstly, the actual prisoners, both technological and legal, are still lacking and still addressed the high demand due to the exact quantity of cybercrime incidents is still massive, especially the extreme CII level of cyber threats requiring practitioners to handle this situation. Moreover, the organization’s essential approach of “appropriate security structure” is still comprehensively available, and the cybersecurity investment requires a high budget for contribution or recovery after facing cyber threats. Therefore, private and government sectors must produce professional practitioners and spread cybersecurity investment conclusively to decrease the damage when faced with cyber threats or encounters cybercrime better than recently. Secondly, as the officer and practitioner under the CSA and CCA framework, I found one significant loophole in the definition of CSA enforced only in the context of “Government Agencies” and “CII” sectors. Understandably, this Act has the specific purpose of being enforced, but when the actual threats happened to some “Government Sector” did not apply the CSA enactment and some large enterprises of the private sector, which possibility concerned the “CII” and request for the emergence of assistance from Thai Cert but Thai Cert has no authority or specific power under CSA into arrangement. Therefore, it is recommended that legislators consider the “expansion” of the definition to expand the comprehensive approach measures to other essential organizations and sectors into inclusive arrangements regarding cyber threat incidents. Thirdly, regarding the previous issues about the cybersecurity investment with essential demand in Thailand society, which should spread this system appropriately. Many cases rely on Government authorities only, but sometimes the Government needs assistance from the Private Sector as this sector requests assistance and cooperation. Therefore, it is suggested that the “Public Private Partnership or PPP” should be addressed and developed into enhancing the practice through the assistance policy, strengthening the prevention measures, and approaching the detection and suppression of cybercrime, including personal data breach circumstances as the actual

partnership for comprehensive operation between private and government sectors.

