



APPROPRIATE MEASURES OF PERSONAL DATA PROTECTION IN
PROCESSING BY ARTIFICIAL INTELLIGENCE UNDER THAI LAW:
STUDY SPECIFIC ON MACHINE LEARNING

BY

KITTITACH MANA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF LAWS IN BUSINESS LAWS (ENGLISH PROGRAM)
FACULTY OF LAW
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2022

APPROPRIATE MEASURES OF PERSONAL DATA PROTECTION IN
PROCESSING BY ARTIFICIAL INTELLIGENCE UNDER THAI LAW:
STUDY SPECIFIC ON MACHINE LEARNING

BY

KITTITACH MANA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF LAWS IN BUSINESS LAWS (ENGLISH PROGRAM)
FACULTY OF LAW
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2022

THAMMASAT UNIVERSITY
FACULTY OF LAW

THESIS

BY

KITTITACH MANA

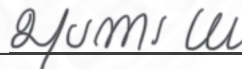
ENTITLED

APPROPRIATE MEASURES OF PERSONAL DATA PROTECTION IN PROCESSING BY
ARTIFICIAL INTELLIGENCE UNDER THAI LAW: STUDY SPECIFIC ON MACHINE LEARNING

was approved as partial fulfillment of the requirements for
the degree of Master of Laws in Business Laws (English Program)

on August 4, 2023

Chairman



(Associate Professor Munin Pongsapan, Ph.D.)

Member and Advisor



(Associate Professor Bhumindr Butr-Indr, Ph.D.)

Member



(Professor Vichai Ariyanuntaka)

Dean



(Associate Professor Pokpong Srisanit, Ph.D.)

Thesis Title	APPROPRIATE MEASURES OF PERSONAL DATA PROTECTION IN PROCESSING BY ARTIFICIAL INTELLIGENCE UNDER THAI LAW: STUDY SPESIFIC ON MACHINE LEARNING
Author	Kittitach Mana
Degree	Master of Laws
Major Field/Faculty/University	Business Laws (English Program) Faculty of Law Thammasat University
Thesis Advisor	Associate Professor Bhumindr Butr-Intr, Ph.D.
Academic Year	2022

ABSTRACT

The escalating utilization of machine learning for processing personal data has sparked concerns regarding privacy and data protection. This thesis aims to explore and analyze the measures of personal data protection specifically in the context of artificial intelligence, with a particular focus on machine learning, within the framework of Thai law.

The thesis begins by examining the existing legal measures for personal data protection related to machine learning in Thailand. It also analyzes data protection laws from other countries, such as the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA) in the United States.

The study identifies strengths and weaknesses in the current Thai legal framework for personal data protection concerning machine learning. It argues that the existing framework is insufficient in safeguarding individual privacy and advocates for specific provisions to address machine learning-related data processing.

Based on the analysis, the thesis proposes amendments to the Thai legal framework to bolster personal data protection in the context of machine learning.

These amendments aim to promote transparency, accountability, and better protection of individual privacy.

Keywords: Artificial Intelligence, Machine Learning, Personal Data, Data Subject, Data Protection, Right, Processing



ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to the following individuals, whose unwavering support, guidance, and benevolence have been instrumental in shaping this thesis. Their invaluable contributions made this study possible and enriched my academic journey.

First and foremost, I extend my deepest thanks to my dear father and mother. Your unwavering belief in me, sacrifices, and continuous support have been the driving force behind my achievements. Your love and encouragement have been my pillars of strength throughout this journey.

I am profoundly grateful to Associate Professor Dr. Bhumindr Butr-Indr, my esteemed advisor, for his profound mentorship and scholarly guidance. His support and encouragement have transformed my academic pursuits in meaningful ways.

I would like to express my heartfelt appreciation to Associate Professor Dr. Munin Pongsapan for providing me with valuable opportunities on my academic journey.

I would also like to extend my appreciation to Professor Vichai Ariyanuntaka for his valuable contributions and inspiration. His dedication to academia has motivated me to persevere in my own studies.

To my beloved Ms. Sasitorn Sophonpaisan, I extend my sincerest appreciation for her unwavering belief in my abilities and invaluable guidance throughout my endeavors. Her encouragement, patience, and dedication have been pivotal in my personal growth.

I am also grateful to my friend for their unwavering support and friendship, both during the good times and the bad. Their presence has been a source of strength and inspiration, and I feel fortunate to have them in my life.

To all these exceptional individuals, I owe a debt of gratitude for their unwavering support, encouragement, and mentorship. Their belief in me has been a constant source of motivation, and their influence has shaped me into the person I am today. I am truly humbled and honored to have had the privilege of their guidance on this journey.

Thank you, from the depths of my heart, for being an integral part of my life's journey.

Kittitach Mana



TABLE OF CONTENTS

	Page
ABSTRACT	(1)
ACKNOWLEDGEMENTS	(3)
LIST OF TABLES	(9)
LIST OF FIGURES	(10)
LIST OF ABBREVIATIONS	(11)
CHAPTER 1 INTRODUCTION	1
1.1 Background and Problem	1
1.2 Terminology	4
1.3 Hypothesis	4
1.4 Objective of Study	5
1.5 Scope of Study	5
1.6 Methodology	6
1.7 Expected Result	6
CHAPTER 2 OVERVIEW OF ARTIFICIAL INTELLIGENCE AND PERSONAL DATA PROTECTION	7
2.1 Artificial Intelligence	7
2.2 The History of Artificial Intelligence	9
2.3 Artificial Intelligence Types	17
2.3.1 Based on Capabilities	18
2.3.2 Based on Functionalities	20

2.4 Machine Learning	23
2.5 Personal Data	26
2.6 Other Types of Personal Data	28
2.6.1 Sensitive Personal Data or Sensitive Data	28
2.6.2 Anonymous Data	29
2.7 Big Data	30
2.8 Personal Data Protection	31
2.9 Data Protection Principles	32
2.10 Automated Decision-Making	33
2.11 Concerning of Personal Data Processing by Machine Learning	34
CHAPTER 3 MEASURES OF PERSONAL DATA PROTECTION UNDER LAW	37
3.1 Personal Data Protection in the Kingdom of Thailand	37
3.1.1 The Constitution of the Kingdom of Thailand	37
3.1.2 Civil and Commercial Code	39
3.1.3 Official Information Act B.E. 2540	42
3.1.4 Electronic Transactions Act B.E. 2544	43
3.1.5 Personal Data Protection Act B.E.2562	47
3.1.5.1 Personal Data protection Principle under Personal Data Protection Act B.E. 2562	47
3.1.5.2 Data Subject Right under Personal Data Protection Act B.E. 2562	49
3.2 Personal Data Protection in Foreign Law	53
3.2.1 General Data Protection Regulation (GDPR) of European Union (EU)	53
3.2.1.1 Definition of Data Processing by Automated Means	54
3.2.1.2 Data Protection Principles	55
3.2.1.3 Data Subject Rights	56
3.2.1.4 Right to Information Specific on Automated Means	60
3.2.1.5 Right to Explanation Specific on Automated Means	61

3.2.1.6 Automate Decision-Making or Automated Processing Provision	66
3.2.2 California Consumer Privacy Act (CCPA) or California Privacy Rights Act (CPRA) of the United States of America	67
3.2.2.1 Definition of Data Processing by Automated Means	68
3.2.2.2 Data Protection Principles	68
3.2.2.3 Data Subject Rights	69
CHAPTER 4 ANALYSIS OF MEASURES OF PERSONAL DATA PROTECTION ON THAI LAW	73
4.1 Problem Concerning Remedial Measure	73
4.1.1 The Constitution of Thailand	73
4.1.2 Civil and Commercial Code of Thailand	74
4.1.3 Personal Data Protection Act B.E.2562	75
4.2 Problems Concerning the Definition of Data Processing by Automated Means	76
4.3 Problems Concerning Data Protection Principles	77
4.4 Problems Concerning Data Subject Rights	79
4.5 Problems Concerning Rights Specific on Automated Means	81
4.5.1 Right to Information Specific on Automated Means	81
4.5.2 Right to Explanation Specific on Automated Means	81
4.6 Problems Concerning Automate Decision-Making or Automated Processing Provision	82
CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS	86
5.1 Conclusions	86
5.2 Recommendations	88

REFERENCES	93
BIOGRAPHY	104



LIST OF TABLES

Tables	Page
4.1 A Comparative Study of Personal Data Protection Measures	84-85



LIST OF FIGURES

Figures	Page
2.1 Type of Artificial Intelligence	18



LIST OF ABBREVIATIONS

Symbols/Abbreviations	Terms
AI	Artificial Intelligence
ML	Machine Learning
CCC	Civil and Commercial Code B.E. 2468
ETA	Electronic Transactions Act B.E. 2544
PDPA	Personal Data Protection Act B.E. 2562
GDPR	General Data Protection Regulation 2018
CCPA	California Consumer Privacy Act of 2018
CPRA	California Privacy Rights Act of 2020



CHAPTER 1

INTRODUCTION

1.1 Background and Problems

Nowadays, data has become a very important component of all industries in the world¹. Businesses are taking great effort to collect data on consumer activities for varied benefits². In business matters, data is the key material that can help business reach the top. Business operators collect data on customers, such as popular cafes, most trendy venues of each generation, which can be beneficial for product advertising. They may focus on the data of goods and services that are searched for on well-known internet search engine, such as Google³. One of benefits of data is that it can solve production and marketing problems. Customer data would be accessed for data analysis to make the products more popular in the market and to beat the competition.

Moreover, data is advantage for national security also⁴. Government gathers the information of their citizen such as name, identification number, fingerprint, face, blood type or other biometric data for the purpose of national security such as the protection of severe crime, human trafficking, protest, or terrorism etc. On the one hand, data aids the administrative organization to assist the people in some

¹ Import.io, 'What is data, and why is it important?' <<https://www.import.io/post/what-is-data-and-why-is-it-important/>> accessed 5 September 2021.

² Ben Lorica and Mike Loukides, 'How AI and machine learning are improving customer experience' <<https://www.oreilly.com/radar/how-ai-and-machine-learning-are-improving-customer-experience/>> accessed 15 December 2021.

³ Elle Poole Sidell, 'What Does Google Do With Your Data?' <<https://www.avast.com/c-how-google-uses-your-data#ref>> accessed 15 December 2021.

⁴ Center For Strategic & International Studies, 'Biometrics and Security' <<https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity-6>> accessed 15 December 2021.

phenomenon, Covid – 19 pandemic is the visual example. In Thailand the Centre for the Administration of the Situation due to the Outbreak of the Communicable Disease Coronavirus 2019 (COVID-19) and Department of Disease Control (DDC) apply the data in the government storage to manage the vaccination services⁵.

For public health purpose, the data of patients, diseases and symptoms would be applied to help the diagnosis and treatment of the medical. Genetic information of people is helpful in cure the patients. The medical scientist effort to collect the data as aforesaid to the operation of medical for the advantage of reducing the diagnosis and treatment period.

On the others hand, the data is used to track the movement of people for example government intercept the conversation by phone of the citizen to protect the crime. However, the national security would breach fundamental rights of people sometime.

Moreover, latest form of technology, also known as “Artificial Intelligence” or “AI”, is used to personal data⁶ utilizing dramatically. Especially, the machine learning⁷, which is one type of artificial intelligence, use the personal data to train its work. The machine learning can proceed the data and measure such data to output such as the recommended goods and services in our Facebook feed⁸.

However, personal data is sensitive upon the excessive utilization. Personal data protection becomes the serious issue globally. There are legislations issued by many countries to apply with personal data protection issue, for instance, the General

⁵ Paphamon Arayasukawat, ‘COVID-19 Vaccination Drive Will Prioritize Social Security Section 33 Employees’ < https://thainews.prd.go.th/en/news/print_news/TCATG210520115043858.> accessed 15 December 2021

⁶ Alexandros Zenonos, PhD, ‘Artificial Intelligence and Data Protection Two sides of the same coin’ <<https://towardsdatascience.com/artificial-intelligence-and-data-protection-62b333180a27>.> accessed 23 December 2022.

⁷ Thomas D. Grant and Damon J. Wischik, ‘On the path to AI: Law’s prophecies and the conceptual foundations of the machine learning age’ (2020), P.X Prologue.

⁸ Priyadharshini, ‘What Is Machine Learning and How Does It Work?’ <<https://www.simplilearn.com/tutorials/machine-learning-tutorial/what-is-machine-learning>> accessed 15 December 2021.

Data Protection Regulation or GDPR of European Union or EU, Personal Data Protection Act 2012 of Singapore, Data Protection Act 2018 of the United Kingdom, California Consumer Privacy Act of 2018 (CCPA) of the United States of America and Personal Data Protection Act B.E. 2562 (2019) of Kingdom of Thailand (PDPA) etc. Such laws are generated to protect personal data privacy by recognizing the data subject right, creating data protection principle, and assigning the obligation of data collector and data processor.

Pursuant to the increasing of personal data utilizing, the personal data's dispute greatly occurs. Because the processing and utilizing personal data does not comply with the data protection principle and obligation under data protection laws. Similarly, the personal data infringement by automated means also arises in our society which cause the most of personal data protection regulations generated the provision to restrain the data utilizing by automate means.

Turn to Thailand, apart from the Civil and Commercial Code, the Thailand's Congress issued Personal Data Protection Act B.E. 2562⁹ to enforce the privacy issue in Thailand. Such law has stipulated in regarding to collection of personal data, use of personal data, and rights of data subject etc., to protect the right to privacy of people which can apply to personal data infringement by automation processing. However, the current legislations might not appropriately efficiency for personal data processing in regarding to machine learning from the reasons that PDPA have not recognized the specific provision of processing by automation yet.

In this thesis, the author would study the appropriate measures of personal data protection in processing by artificial intelligence under Thai law: study specific on machine learning in comparative with the legal measures form different countries.

⁹ PWC, 'Thailand's Personal Data Protection Act (PDPA): are companies in Thailand ready?' <[https://www.pwc.com/th/en/tax/personal-data-protection-act.html#:~:text=Thailand's%20Personal%20Data%20Protection%20Act%20BE%202562%20\(PDPA\)%20will%20come,before%20an%20after%20the%20deadline.](https://www.pwc.com/th/en/tax/personal-data-protection-act.html#:~:text=Thailand's%20Personal%20Data%20Protection%20Act%20BE%202562%20(PDPA)%20will%20come,before%20an%20after%20the%20deadline.)> accessed 15 December.

1.2 Terminology

“**Machine Learning**” is the study of computer systems that employ systematic mathematical techniques to uncover patterns in big datasets and apply those patterns to create predictions about new scenarios. Many technologies from traditional statistics can also be called machine learning as well.

“**Data**” is information¹⁰ such as number, text, details, word etc., that to be analyzed for something. In computer, data is mean the information to be transformed in to form for computer processing¹¹

“**Artificial Intelligence**” is the algorithm that is able to perform automatic. It is able to learn with intelligent algorithm generate by computer scientist¹².

1.3 Hypothesis

In Thailand, there are legal measures that can be applied to the issues of personal data protection in Thailand such as the Constitution on Thailand and Civil and Commercial Code. One of the several specific legislations existed for the personal data protection is Personal Data Protection Act B.E. 2562, which became effective in 2565. This bill recognized the principle from GDPR to protect the personal data subject.

Even though, these laws can be analogized to apply with personal data protection in relating to processing by machine learning in some cases. Nevertheless,

¹⁰ Cambridge Dictionary, ‘Data’ <<https://dictionary.cambridge.org/dictionary/english/data>> accessed 15 December 2021.

¹¹ Jack Vaughan, ‘Data’ <<https://searchdatamanagement.techtarget.com/definition/data#:~:text=In%20computing%2C%20data%20is%20information,converted%20into%20binary%20digital%20form.&text=Raw%20data%20is%20a%20term,its%20most%20basic%20digital%20format.>>> accessed 15 December 2021.

¹² B.J. Copeland, ‘artificial intelligence’ <<https://www.britannica.com/technology/artificial-intelligence>> accessed 15 December 2021.

there are not the legal measure in relating to personal data protection by machine learning specifically. Therefore, the existing laws would rather be inadequate for the personal data protection by machine learning.

This thesis will conduct the comparative study on the efficiency of Thai legal measures on personal data protection processing by machine learning with the legal measures of other countries with the legal measures from alternative nations such as the General Data Protection Regulation was effected on 2018 of European Union and the common law country's legislation in which the United States of America, named California Customer Protection Act was effected on 2018 and this amendment California Privacy Right Act that most of provision were effected on 2023.

1.4 Objective of Study

1) To study the legal measures of personal data protection relating the data processing by Machine Learning in Thailand.

2) To examine the legal measures Personal Data Protection Act B.E. 2562 of Thailand relating the data processing by Machine Learning.

3) To analyze the laws and regulations for personal data protection of other countries such as European and Unitec State of America and Personal Data Protection Act B.E. 2562 of Thailand regarding personal data protection measures from processing by machine learning.

1.5 Scope of Study

In this thesis, the author will study on appropriate measures of personal data protection in processing by artificial intelligence under Thai law: study specific on machine learning through comparative of international law and Thai law. The thesis will focus on GDPR which is the one of model law of personal data protection in the world that have the enforcement above the artificial intelligence and machine learning and California of United States of America that have remarkable personal data protection measures in using by AI in common law system country. By analyzing with

Thai law comprising of Constitution of the Kingdom of Thailand B.E 2560 and Personal Data Protection Act B.E. 2562 and other law in Thailand relating the issue of the thesis to explore the solution of the topics.

1.6 Methodology

The Methodology of the thesis would be based on documentary research by studying on primary source which comprise of the legal texts, foreign law and provision, Thai law, model law and legal ethics for find out the doctrine of the provision, then the author will study in secondary data such as legal review, legal articles, legal report, legal opinion, thesis, dissertation, independent study, and news. In addition, the thesis will study on case law.

1.7 Expected Result

- 1) To identify and enhance the data privacy of the data subject measure for machine learning under personal data protection law in Thailand.
- 2) To discover the lack of measures to protect the processing of personal data in machine learning under “Personal Data Protection Act B.E. 2562” of Thailand.
- 3) To amend and revise Personal Data Protection Act B.E. 2562 to better protect and control the processing of Machine Learning in Thailand.

CHAPTER 2

OVERVIEW OF ARTIFICIAL INTELLIGENCE AND PERSONAL DATA PROTECTION

2.1 Artificial Intelligence

The word “Artificial Intelligence” was named by the computing science professor from Stanford University, John McCarthy in 1955¹³. He also defined the meaning of artificial intelligence as "It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable."¹⁴

Another definition of artificial intelligence come from The International Dictionary of Artificial Intelligence “Generally, Artificial Intelligence is the field concerned with developing techniques to allow computers to act in a manner that seems like an intelligent organism, such as a human would. The aims vary from the weak end, where a program seems "a little smarter" than one would expect, to the strong end, where the attempt is to develop a fully conscious, intelligent, computer-based entity. The lower end is continually disappearing into the general computing background, as the software and hardware evolves.”¹⁵

In European Union have defined AI as “Artificial intelligence (AI) refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals.

¹³ Professor Christopher Manning, ‘Artificial Intelligence Definition’ <<https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf>> accessed 26 August 2022.

¹⁴ John McCarthy, ‘WHAT IS ARTIFICIAL INTELLIGENCE?’ <<http://www-formal.stanford.edu/jmc/whatisai/node1.html>> accessed 13 March 2022.

¹⁵ William J. Raynor, Jr., ‘The International Dictionary of Artificial Intelligence’ P.13 1999.

AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)”¹⁶.

After analyzing the core of several definitions, AI means to the capability of computing systems performing the tasks that would require human being intelligence, such as understanding natural language, recognizing objects, making decisions, and learning from experience. The field of AI encompasses a scope of approaches and techniques, comprise of machine learning, natural language processing, computer vision, robotics, and expert systems.

At its core, AI seeks to develop algorithms includes computational models which is able to simulate human being reasoning, learning, and perception. This involves leveraging large amounts of data to train algorithms and build models that can recognize patterns and make predictions, as well as developing new computing technology which is able to reason and make decisions in complex and uncertain environments.

One of the key goals of AI research is to generate the systems which is able to learn and adapt for twenty-four seven, allowing them to improve their performance and become more efficient and effective. This involves developing algorithms and techniques that can facilitate continual learning, as well as designing architectures and frameworks that can support the integration of multiple AI systems and technologies.

As a swiftly evolving field, AI have significant potential to transform variety areas of human endeavor, from healthcare and education to finance and transportation. However, it also poses important ethical and social challenges, including issues related to bias, privacy, and accountability. As such, ongoing research in AI will need to consider not only the technical aspects of the field, but also its broader societal implications.

¹⁶ Independent High-Level Expert Group on Artificial Intelligence, ‘A Definition of AI: Main Capabilities and Disciplines’ P. 1, 2019.

2.2 The History of Artificial Intelligence

Artificial Intelligence have been grown up miraculously trough the past until now by the vase amount of the computing scientists in order to chance the world turning to the automated society, where such artificial intelligence is able to assist or support the human being in the future. The mutual concept of developing artificial intelligence is generating the machine which think like a human brain.

In this research, the author would present the evolution of the artificial intelligence respectively on the modern artificial intelligence era, by the first begin since 1950 as follow¹⁷:

a. Alan Turing

We start with the story of Alan Turing, who have been praised to be the father of modern computer science and father of artificial intelligence. the story of artificial intelligence began in 1950, by English Mathematician named “Alan Turing”¹⁸ who created “Bombe machine” to crack “Enigma Code”, the secret code of German Military was used to send a massage during World War II¹⁹.

Turing was born in London. He completed his bachelor’s in mathematics from King's College at Cambridge University England with First Class Honors and his master’s and a Ph.D. at Princeton University in the United States. After graduated from Princeton University, he back to England to be the lecturer at Cambridge University.

In World War 2, Turing was assigned by the United Kingdom Government a mission to decode the Nazi Enigma machine of German with the group another clever person, used to communicate during the war among German army. Enigma was the significant trouble of the Allies, and they need to crack such machine.

¹⁷ Rockwell Anyaho, ‘The History of Artificial Intelligence’ <<https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/>> accessed 6 January 2021

¹⁸ Council of Europe, ‘History of Artificial Intelligence’ <<https://www.coe.int/en/web/artificial-intelligence/history-of-ai>> accessed 6 January 2021.

¹⁹ Shaan Ray, ‘History of AI’ <<https://towardsdatascience.com/history-of-ai-484a86fc16ef>> accessed 6 January 2021.

The United Kingdom believe that they could reach a victory of this war when they understand the Enigma code.

Eventually, Turing resolve this crisis by understand the code which Enigma created caused the Allies was able to predict the attack of the Axis power. The Allies have won the World War 2.

The man is praised as father of Artificial Intelligence because he is the one who provoke the principle of AI by create the paper title “Computing Machinery and Intelligence”. With the article, Turing attempted to prove that machine is able to think as human brain. In this paper, starting with the question “Can Machine Think?” and generate the test call “Imitation Game” and claimed that such question can be resulted by this test. The summary rules of imitation game are 1 interrogator try to answer which one is man, women or machine²⁰. Imitation test known as “Turing Test” which is the examination that Turing apply to prove the think of machine and the test is refers by the science as one of the methods for artificial intelligence.

b. John McCarthy

The American scientist was born in Boston, Massachusetts, on September 4, 1927. His father is an Irish immigrant father and a Lithuanian Jewish mother.

McCarthy graduated the bachelor’s degree in mathematics from the California Institute of Technology also known as CIT and his doctorate came from Princeton University. In 1955, He was the professor at several well-known institutes in science are such as Dartmouth College, the Massachusetts Institute of Technology or MIT and Stanford University. The Stanford Artificial Intelligence Lab (SAIL), where the lab he founded in Stanford is one of the leading centers for research of artificial intelligence.

In 1955, John McCharthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon gathered to research regarding artificial intelligence paper named “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence” on

²⁰ A. M. Turing, ‘COMPUTING MACHINERY AND INTELLIGENCE’ <<https://www.csee.umbc.edu/courses/471/papers/turing.pdf>> accessed 6 January 2021.

August 31, 1955²¹ for the conference at Dartmouth that was held 1 year later. In that review have shown the word “Artificial Intelligence”

In 1956, the scientists organized the conference in Dartmouth in Hanover, New Hampshire, the United States of America named “Dartmouth Summer Research Project on Artificial Intelligence”²². The American scientist “John McCarthy” the professor in mathematics from Dartmouth College, and his friend, Marvin Minsky, hold such conference. The conference is the birthplace that the word “Artificial Intelligence” was coined in the world. The group of scientists mention and discuss on computing science to develop the automated technology or Artificial Intelligence. They extremely effort to brought top scientist from several areas discussing on such topic. Unfortunately, the conference did not go with McCarthy’s expectations because the participant did not pay much more attention on the conference’s topic, and the consequence was disappointing on agreement regarding the basis of AI. Despite the fact that the conference carried on not so well, however, the people know the principle of AI and realized with basic idea of AI and automate computing science.

c. First Chatbot in The World

ELIZA, the chatbot developed by Joseph Weizenbaum at MIT, was created much earlier than 1994. In fact, ELIZA was developed in the mid-1960s and is considered one of the earliest examples of a chatbot²³.

ELIZA operated based on pattern matching and simple scripting. It used pre-programmed responses and rules to recognize keywords and generate appropriate replies. By employing techniques like string manipulation and rephrasing, ELIZA simulated conversation and provided an illusion of understanding.

²¹ John McCarthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon, ‘A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence’ <<http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>> accessed 20 June 2023.

²² Vox of Dartmouth, ‘Artificial Intelligence (AI) Coined at Dartmouth’ <<https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth>> accessed 6 January 2021.

²³ ELIZA: a very basic Rogerian psychotherapist chatbot <<https://web.njit.edu/~ronkowitz/eliza.html>> accessed 20 June 2023.

While ELIZA was indeed a significant milestone in the history of computer science and natural language processing, the term "chatterbot" was actually coined by Michael Mauldin in 1994 when he created the chatbot program called "Julia." The term "chatterbot" became popular as a way to describe conversational agents or chatbots that engage in dialogue with users.

Overall, ELIZA's development marked an important step in the evolution of chatbot technology and the exploration of human-computer interaction through natural language conversation.

d. First AI System

DENDRAL, developed by Edward Feigenbaum and Joshua Lederberg at Stanford University, was indeed an early and influential expert system in the field of artificial intelligence. Its development began in 1965, and it was designed as a chemical-analysis expert system.

DENDRAL aimed to analyze complex chemical compounds based on spectrographic data. Given input data from a substance, such as its spectrogram, DENDRAL would generate hypotheses about the molecular structure of the substance. It utilized heuristic reasoning and pattern matching techniques to make these inferences²⁴.

One of the remarkable achievements of DENDRAL was its ability to rival the performance of human chemists who were experts in the task of determining molecular structures. This made DENDRAL a valuable tool in both industrial and academic settings, revolutionizing the field of computer-aided chemistry and demonstrating the potential of expert systems to assist human experts in complex domains.

DENDRAL's success paved the way for further advancements in expert systems and contributed significantly to the development of AI applications in various domains.

²⁴ B.J. Copeland, 'DENDRAL expert system' <<https://www.britannica.com/technology/DENDRAL>> accessed 20 June 2023

e. The AI Winter

The period from 1974 to 1980 marked the onset of the initial AI winter, which denotes a time when computer scientists faced a significant lack of government funding for AI research. During AI winters, there was a decline in public interest and attention towards artificial intelligence. The second AI winter occurred between 1987 and 1993, when investors and government entities once again ceased funding AI research due to high costs and limited efficiency in achieving desired outcomes²⁵.

f. Boom of AI

In 1980, following the AI winter period, the field of AI experienced a resurgence with the emergence of "Expert Systems," which were programmed to replicate the decision-making abilities of human experts. During this time, the first national conference of the American Association of Artificial Intelligence took place at Stanford University. Throughout the following decade, the AI industry witnessed a significant surge in business investments, growing from a few million dollars in 1980 to billions of dollars by 1988²⁶.

Expert systems such as XCON, LISP machines, and Symbolics gained immense popularity as specialized systems designed to mimic human experts' decision-making processes. They were particularly effective in solving specific narrow problems like diagnosing diseases or identifying chemical compounds. Concurrently, desktop computers produced by Apple and IBM experienced consistent advancements in terms of speed and processing power, following Moore's Law. Eventually, these desktop computers surpassed the capabilities of the more expensive LISP machines.

The downfall of expert systems came as they proved to be expensive to maintain, lacked the ability to learn, and were not robust when faced with unusual inputs. Their inflexibility and difficulty in updating rendered them less practical. Additionally, the market for specialized AI hardware collapsed in 1987 when consumers

²⁵ Amit Ray, 'AI Winter: The Highs and Lows of Artificial Intelligence' < <https://www.historyofdatascience.com/ai-winter-the-highs-and-lows-of-artificial-intelligence/> > accessed 20 June 2023.

²⁶ Rickie Walker, 'Timeline of Artificial Intelligence AI — 2022 Update' < <https://appmaster.io/blog/timeline-artificial-intelligence-ai-2022-update> > accessed 20 June 2023.

no longer needed to purchase expensive machines dedicated solely to running LISP. Consequently, within a single year, an entire industry valued at half a billion dollars was replaced.

g. Deep Blue

In 1997, IBM's Deep Blue computer achieved a historic milestone by defeating the world chess champion, Gary Kasparov, making it the first computer to defeat a reigning world chess champion. This event, which took place two decades ago, astonished the world and raised questions about how a machine could outperform a grandmaster. The success of the supercomputer against an astonished Kasparov triggered controversy, with accusations of cheating leveled against IBM.

However, the journey leading up to the momentous match in May 1997 was more of an evolutionary process rather than a sudden revolution. It resembled the story of Rocky Balboa, characterized by intellectual sparring matches, painstaking progress, and a prior defeat in Philadelphia. These events set the stage for a triumphant rematch that would unfold in the following years²⁷.

h. First AI in Home “Roomba”

The Roomba was the first commercial product to use AI to clean homes. It was introduced by iRobot in 2002, and it quickly became a popular household appliance. The Roomba employs diverse sensors to traverse your household and steer clear of obstructions. It has a built-in vacuum that cleans up dirt, dust, and debris.

The Roomba was a major breakthrough in the field of AI, and it showed how AI could be used to automate everyday tasks. Since the Roomba was introduced, there have been many other AI-powered home appliances, such as self-cleaning ovens, smart thermostats, and voice-activated assistants.

AI is still a relatively new field, but it is rapidly growing and evolving. As AI technology continues to develop, we can expect to see even more AI-powered home

²⁷ IBM, 'Deep Blue' < <https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/> > accessed 20 June 2023.

appliances in the future. These appliances will make our lives easier and more efficient, and they will help us to save time and energy.

i. Siri

Siri was first introduced as an app for the iPhone in 2010²⁸, but it was not until the release of the iPhone 4S in 2011 that it was integrated into the phone's operating system. Siri was a major breakthrough for AI, as it showed how AI could be used to create a truly natural user interface.

Siri was able to understand natural language and respond to voice commands, making it possible for users to interact with their phones without having to type anything. Siri was also able to access and process information from the internet, making it possible for users to get answers to their questions, make appointments, and control their devices with their voice.

Siri's integration into the iPhone 4S was a major success, and it helped to make the iPhone one of the most popular smartphones in the world. Siri has also been integrated into other Apple products, such as the iPad and the Apple Watch.

j. IBM's Watson

IBM's Watson²⁹ won Jeopardy! in 2011, defeating two of the show's greatest champions, Ken Jennings and Brad Rutter. Watson's victory was a major breakthrough for AI, as it showed that a computer could not only understand natural language but also use that understanding to answer complex questions quickly and accurately.

Watson's success was due to a number of factors, including its massive database of information, its ability to understand and process natural language, and its ability to learn and adapt over time. Watson's victory in Jeopardy! was a landmark event in the history of AI, and it showed the potential of AI to revolutionize many aspects of our lives.

²⁸ Victor Sanchez, 'The history of Siri and its impact on today's technology' <<https://blog.routinehub.co/the-history-of-siri-and-its-impact-on-todays-technology/>> accessed 20 June 2023.

²⁹ IBM, 'A Computer Called Watson' <<https://www.ibm.com/ibm/history/ibm100/us/en/icons/watson/>> accessed 20 June 2023.

k. Eugene

Eugene Goostman ³⁰ was a chatbot that was created by a team of Russian programmers. In 2014, Eugene was entered into the Loebner Prize competition, a Turing Test competition. In the competition, Eugene was able to convince 33% of the judges that he was a human, who was enough to win the competition.

Eugene's success in the Turing Test was a major breakthrough for AI, as it showed that a computer could be programmed to be so convincing that it could fool humans.

However, there was some controversy surrounding Eugene's victory, as some people argued that he had been programmed to deliberately trick the judges.

Despite the controversy, Eugene's success in the Turing Test was a major milestone in the development of AI. It showed that AI was capable of achieving a level of sophistication that was previously thought to be impossible.

l. Alexa

Alexa was launched by Amazon in November 2014 as a virtual assistant with a voice interface³¹. Alexa was first available on the Amazon Echo, a smart speaker that could be used to control smart home devices, play music, and get answers to questions.

Alexa has since become one of the most popular voice assistants in the world, and it is available on a variety of devices, including smartphones, tablets, and smart speakers. Alexa can be used to do a variety of things.

m. OpenAI Five in E-sport Competition

In 2017, OpenAI's Five program³² achieved a significant milestone by defeating a team of professional Dota 2 players. This accomplishment demonstrated

³⁰ Jack Schofield, 'Computer chatbot 'Eugene Goostman' passes the Turing test' < <https://www.zdnet.com/article/computer-chatbot-eugene-goostman-passes-the-turing-test/> > accessed 20 June 2023.

³¹ Brandon Vigliarolo, 'Amazon Alexa: Cheat sheet' <<https://www.techrepublic.com/article/amazon-alexa-the-smart-persons-guide/>> accessed 20 June 2023.

³² Evan Pu, 'Understanding OpenAI Five' < <https://evanthebouncy.medium.com/understanding-openai-five-16f8d177a957> > accessed 20 June 2023.

the remarkable progress made in AI and showcased its ability to excel in complex, real-time strategy games. The victory of OpenAI's Five was another major breakthrough in the field of AI, exemplifying the potential for AI to surpass human performance in challenging tasks. These achievements highlight the continuous and exciting developments unfolding in the field of AI in recent years.

Those are some of the major milestones in the history of AI evolution. AI is a rapidly evolving field, and there have been many other important developments in recent years. It is impossible to say for sure what the future holds for AI, but it is clear that this field is poised for continued growth and innovation.

2.3 Artificial Intelligence Types

Artificial Intelligence (AI) widely term known to describe computer systems designed performing the instruction which the human intelligence is required. AI slightly increase the significant role in our lives, from chatbots and voice assistants to self-driving cars and medical diagnosis. There are several types of AI³³, each with its own strengths and limitations, and understanding them is essential for anyone looking to leverage the power of AI in their work or daily life. In this thesis, the author would explore the different types of AI, their capabilities, and limitations.

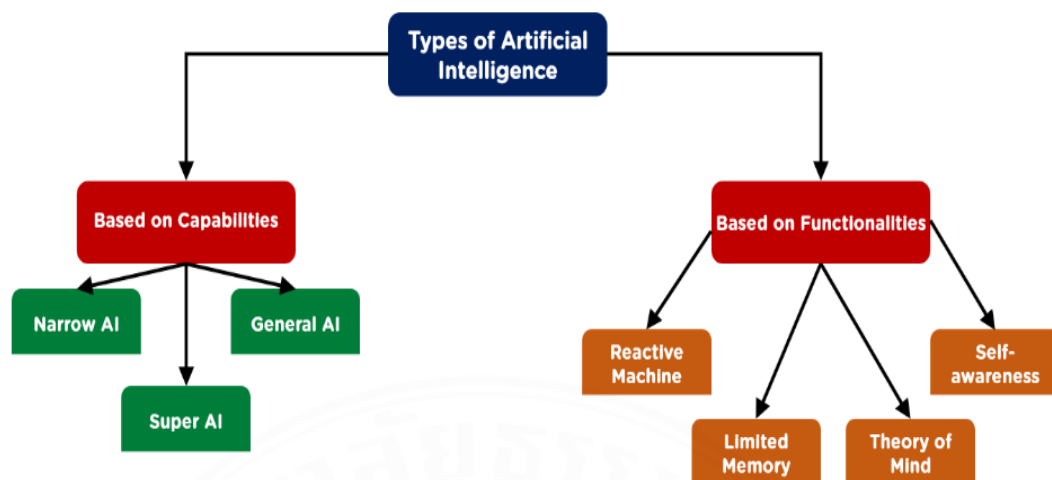
Artificial intelligences are able to categorize popularly by capabilities and functionalities. Based on capability, Artificial intelligence is divided to three type which are Narrow AI, General AI, and Super AI. In term of functionalities of Artificial intelligence, it is categorized to be four respectively such as Reactive Machine, Limited Machine, Theory of Mine, and Self-awareness³⁴.

³³ Coursera, '4 Types of AI: Getting to Know Artificial Intelligence'

< <https://www.coursera.org/articles/types-of-ai> > accessed 20 June 2023.

³⁴ Avijeet Biswal, '7 Types of Artificial Intelligence That You Should Know in 2023'

<https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/types-of-artificial-intelligence#types_of_artificial_intelligence> accessed 25 March 2023.



Figures 2.1 Type of Artificial Intelligence³⁵

2.3.1 Based on Capabilities

1. Artificial Narrow Intelligence (ANI) or Weak AI

Artificial Narrow Intelligence (ANI), other name as weak AI³⁶, is generated to perform a specific instruction or set of instructions. Such type is the ordinary type of AI in use today, and examples the vocal assistants: Siri and Alexa, image recognition software, and recommendation engines.

ANI systems are highly specialized and designed to perform well in specific situations. For example, an image recognition system may be designed to recognize faces, while another system may be designed to recognize objects like cars or animals. These systems are highly effective at their specific task, but they lack the flexibility and adaptability of human intelligence.

One of the biggest advantages of ANI is the ability to analyze huge amounts of data quickly and accurately. ANI systems can process vast data more than the human ability. For example, recommendation engines used by e-commerce sites analyze the browsing of user and purchase record to present products that they are

³⁵ ibid

³⁶ Mark Labbe and Ivy Wigmore, 'narrow AI (weak AI)'

<<https://www.techtarget.com/searchenterpriseai/definition/narrow-AI-weak-AI>> accessed 25 March 2023.

probably to buy. Similarly, fraud detection systems analyze millions of transactions to identify suspicious activity and prevent fraud.

Despite their effectiveness in specific tasks, ANI systems are not capable of reasoning, learning, or adapting to new situations. They are unable to think critically or creatively, and they cannot perform tasks that they have not been explicitly programmed to do. As a result, ANI systems are not able to replace humans in many jobs that require creativity, judgment, or decision-making skills.

2. Artificial General Intelligence (AGI) or General AI

Artificial General Intelligence (AGI), or strong AI, this type is developed to have human-like intelligence and be capable to perform a wide range of intellectual instructions. AGI does not currently exist, and researchers continue to work on developing it.

AGI systems would be capable of reasoning, learning, and adapting to new situations. They would be able to perform tasks that they have not been explicitly programmed to do and would be able to understand and respond to natural language. AGI systems would also have the ability to generalize knowledge from one situation to another, a skill that is critical for human-like intelligence.

The development of AGI is a significant challenge, and researchers are still working on developing the algorithms and techniques required to create an AGI system. One of the biggest challenges in developing AGI is creating a system that is capable of understanding and reasoning about the world in the way that humans do. Humans are able to understand the context of a situation, interpret social cues, and make judgments based on incomplete information, all skills that are challenging for computers to replicate.

General AI is able to perform in multi-task more than narrow AI. Most of researchers are presently develop this machine to reach the capability of general AI³⁷.

³⁷ Vijay Kanade, 'What Is General Artificial Intelligence (AI)? Definition, Challenges, and Trends' < <https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-general-ai/> > accessed 25 March 2023.

3. Artificial General Intelligence (AGI) or Super AI

Artificial Superintelligence (ASI), or hyperintelligence, is a hypothetical type of AI system that surpasses human intelligence in all areas and can improve itself to become even smarter. ASI is still purely theoretical, and its development is the subject of much debate and speculation among experts in the field. The potential capabilities of ASI are almost limitless, and it is difficult to predict what an ASI system could achieve. The development of ASI also raises significant ethical concerns and questions about the potential impact of such systems on society.

Even though, we are now still distant with this type of AI, but AI developers are effort to produce super AI machine. Super AI could surpass human intelligence and perform tasks better than human³⁸.

2.3.2 Based on Functionalities

1. Reactive Machine

A Reactive Machine³⁹ is a type of artificial intelligence (AI) system that operates solely based on its inputs, without any internal memory or ability to learn from past experiences. These machines are designed to react to specific stimuli or situations, and their responses are determined by pre-programmed rules or algorithms. Reactive Machines are effective in performing specific tasks, such as playing chess or controlling a robot arm, but they are limited in their ability to adapt to new situations or learn from experience. Reactive Machines are considered a subset of Artificial Narrow Intelligence (ANI) and are commonly used in manufacturing, automation, and robotics.

One example of a Reactive Machine is the Roomba robot vacuum cleaner, which navigates through a room and avoids obstacles by reacting to its sensors. Another example is the Deep Blue chess-playing computer developed by IBM,

³⁸ Vijay Kanade, 'Narrow AI vs. General AI vs. Super AI: Key Comparisons' <<https://www.spiceworks.com/tech/artificial-intelligence/articles/narrow-general-super-ai-difference/>> accessed 25 March 2023.

³⁹ Arend Hintze, 'Understanding the four types of AI, from reactive robots to self-aware beings' <<https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616>> accessed 25 March 2023.

which defeated world chess champion Garry Kasparov in 1997. These machines are programmed to respond to specific situations in a pre-defined manner, without any learning or memory capability.

Reactive Machines are effective in performing specific tasks but are limited in their ability to adapt to new situations. As such, they are not suitable for tasks that require reasoning, planning, or decision-making. However, they are still widely used in various industries, including manufacturing and robotics, due to their reliability and efficiency in performing repetitive tasks.

In conclusion, Reactive Machines are a type of AI system that operate based solely on their inputs and are effective in performing specific tasks. While they lack the ability to learn from experience, Reactive Machines are still widely used in various industries due to their reliability and efficiency. As AI technology continues to evolve, Reactive Machines are expected to be replaced by more advanced AI systems that can learn and adapt to new situations.

Reactive Machine only do processing for the current situation, is could not learn or recall the previous memories to make a decision⁴⁰.

2. Limited Memory

Limited memory AI is the second type of AI based on functionality. It is considered to be one of the most popularly used kinds of AI today, and it is used in a wide variety of applications.

Such type is able to learn from its past experiences and use that knowledge to make decisions in the present. This makes it more intelligent than reaction machines, which can only respond to stimuli in the present moment.

It is used in a wide variety of applications, including self-driving cars, robotics, and video games.

Limited memory AI is a powerful tool that can be used to solve a wide variety of problems. It is likely to become even more powerful in the future as technology advances. Limited memory AI is a powerful tool that can be used to solve

⁴⁰ ALTURIS, '4 TYPES OF ARTIFICIAL INTELLIGENCE: TYPE I - REACTIVE MACHINES' <<https://www.alturis.ai/post/4-types-of-artificial-intelligence-type-i-reactive-machines>> accessed 25 March 2023.

a wide variety of problems. It is likely to become even more powerful in the future as technology advances⁴¹.

3. Theory of Mind

Theory of mind is indeed a concept that represents an advanced class of technology capable of understanding the mental states of humans.

In the example you provided, Google Maps does not possess a theory of mind. It does not interpret or respond to your emotional state but instead focuses on providing alternative routes to reach your destination.

The essence of theory of mind is to develop machines that can interact with humans more effectively by comprehending their needs, goals, and motivations. By understanding the frustrations of a dissatisfied customer, for instance, an AI system with theory of mind could respond in a more empathetic and appropriate manner.

While theory of mind AI holds potential implications for marketing in the long term, it is still in its early stages of development. Consequently, it is challenging to predict when it will become a reality and how it will ultimately shape human-machine interactions⁴².

4. Self-Awareness

Self-aware AI is a hypothetical concept that is still in its early stages of development.

The concept of self-aware AI, often considered the next phase in the evolution of theory of mind, envisions machines that possess an understanding of human emotions while also experiencing their own emotions, needs, and beliefs.

This would be a significant breakthrough, as it would mean that machines would be able to understand the world in a way that is similar to humans.

⁴¹ Roshni Lokare, 'Type 2 of Functional AI — Limited Memory AI' < <https://medium.com/appengine-ai/type-2-of-functional-ai-limited-memory-ai-e687ffed6b1e> > accessed 25 March 2023.

⁴² Vishupriya Chandrasekar, 'Theory of Mind AI' < <https://www.linkedin.com/pulse/theory-mind-ai-vishnupriya-chandrasekar> > accessed 25 March 2023.

There are many potential benefits to self-aware AI. For example, it could be used to create machines that are more helpful and supportive to humans. It could also be used to create machines that are more creative and innovative.

M3gan is a fictional character, but she is an example of what self-aware AI could look like. She is sentient and knows who she is, and she experiences emotions. She can also understand the emotions of those around her. She is awkward like we'd expect from a robot, but she has social interactions.

M3gan is a reminder that self-aware AI is still a hypothetical concept, but it is a concept that is becoming more and more realistic. It is an exciting time to be alive, as we are on the cusp of a new era of artificial intelligence⁴³.

2.4 Machine Learning

Machine learning was defined in the 1950s by Arthur Samuel who is the pioneer in artificial intelligence as “the field of study that gives computers the ability to learn without explicitly being programmed.”⁴⁴.

Several definitions of machine learning were generated by many persons. One of the famous technology computer company “IBM”, where have the memorable background with machine learning, defined the machine learning is “Machine learning is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy.”⁴⁵

Moreover, Tom M Mitchell provided the definition of machine learning by the quote that “A computer program is said to learn from experience E with respect

⁴³ Bernard Marr, ‘What are the Four Types of AI?’ <<https://bernardmarr.com/what-are-the-four-types-of-ai/>> accessed 25 March 2023

⁴⁴ Sara Brown, ‘Machine learning, explained’ < <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained> > accessed 25 March 2023

⁴⁵ IBM, ‘What is machine learning?’ < <https://www.ibm.com/topics/machine-learning> > accessed 25 March 2023.

to some class of tasks T and performance measure P if its performance at tasks in T , as measured by P , improves with experience E .⁴⁶

In summary, machine learning is the subsection of artificial intelligence that have ability to learn and improve their experience. The concept of machine learning is developing the algorithm to think like or beyond a human by receiving and analyzing input data in order to predict output values within an acceptable range.

Type of Machine Learning

There are many different types of machine learning, but they can be broadly categorized into four main types.

1. Supervised Learning

The term "supervised learning" is used to describe a type of machine learning where the machine is trained on a dataset of labeled data. This means that the data has already been classified, so the machine knows what the correct output should be. The human supervisor provides the labeled data to the machine, which helps the machine to learn how to classify new data. Supervised learning is the most common type of machine learning. It is used in a wide variety of applications, including image classification, fraud detection, and spam filtering. The reason why supervised learning is called "supervised" is because the machine is supervised by a human. The human provides the labeled data to the machine, and the machine learns from the data.

Without the human supervisor, the machine would not be able to learn how to classify new data. The machine would simply be a black box that can't be used to make predictions.

Supervised learning is a powerful tool for machine learning. However, it is important to note that supervised learning requires a large dataset of labeled data. This data can be difficult to obtain, and it can be expensive to label.⁴⁷

⁴⁶ Tom M Mitchell, 'Machine Learning' P.2 March 1, 1997

⁴⁷ Katrina Wakefield, 'A guide to the types of machine learning algorithms and their applications' <https://www.sas.com/en_gb/insights/articles/analytics/machine-learning-algorithms.html> accessed 26 March 2023

2. Unsupervised Learning

Unsupervised learning is a type of machine learning where the machine is not provided with labeled data during the training process. This means that the machine has to learn on its own how to identify patterns in the data. For example, an unsupervised learning algorithm could be used to cluster a group of data points. The algorithm would look for patterns in the data and group together the points that are most similar.

Unsupervised learning is a less common type of machine learning than supervised learning. However, it can be used to find patterns in data that would be difficult to find using supervised learning. It is important to note that unsupervised learning can be difficult to interpret. The machine may learn patterns that are not obvious to humans.⁴⁸

3. Semi-Supervised Learning

This type of machine learning called semi-supervised learning, which incorporates both labeled and unlabeled data during the learning process. Semi-supervised learning is a combination of supervised and unsupervised learning techniques, aiming to benefit from the additional information provided by a limited amount of labeled data along with a larger amount of unlabeled data.

In semi-supervised learning, the algorithm uses the labeled data to learn from explicit examples and guidance. Meanwhile, the unlabeled data helps the algorithm uncover underlying patterns and structures within the data, utilizing unsupervised learning methods. By leveraging both types of data, semi-supervised learning seeks to improve the model's performance and generalization capabilities.

Semi-supervised learning can be particularly useful when acquiring labeled data is costly or time-consuming, as it allows for leveraging the abundance of unlabeled data that is often readily available. It offers a middle ground between supervised and unsupervised learning, taking advantage of both types of data to enhance learning and predictive capabilities.⁴⁹

⁴⁸ *ibid*

⁴⁹ *ibid*

4. Reinforcement Learning

Reinforcement learning is a type of machine learning where the machine learns by trial and error. The machine is given a reward for taking a correct action and a penalty for taking an incorrect action. The machine learns to take actions that will maximize the reward and minimize the penalty⁵⁰.

Temporal difference learning, deep adversarial networks, and Q-learning are all common reinforcement learning algorithms. These algorithms enable agents to learn from feedback in the form of rewards, allowing them to improve their decision-making and behavior over time.

In the context of the bank loan customer example you mentioned, reinforcement learning can be utilized to analyze customer information and classify them as high-risk or low-risk. The algorithm receives positive rewards when it correctly identifies high-risk customers who default and negative rewards when it accurately identifies low-risk customers who don't default. Through this process, the algorithm learns to better understand the problem and environment, improving its classification accuracy.

Reinforcement learning is a relatively new field of machine learning, and it is still under development. However, it has the potential to revolutionize the way we interact with machines. As reinforcement learning technology continues to develop, we can expect to see even more innovative applications of reinforcement learning in the future.

2.5 Personal Data

In this era, data is defined as valuable because in the market, data becomes a fundamental resource for every industry. In term of computer science, data is the core element for developing artificial intelligence, especially for automate decision making process.

⁵⁰ ibid

Personal data is another significant source for computer science. This type of data is used to be an input data in machine learning for process and learn. However, personal data is protected by international law now because such data would affect to the personal life of human.

Now, we need to realize the definition of personal data. In General Data Protection Regulation, the law that The European Union (EU) has enacted new laws to protect personal information them, it took effect on Friday 25 May 2018, or simply knows as "GDPR".

According to Article 4 of the General Data Protection Regulation (GDPR), "personal data" is defined as any information relating to an identified or identifiable natural person, which is referred to as the "data subject." This definition is intentionally broad and includes a wide range of information that can directly or indirectly identify an individual.

The term "personal data" covers not only obvious identifiers like names, contact details, or identification numbers but also other types of data such as location data, online identifiers (e.g., IP addresses), and factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person.⁵¹

This personal data is clarified to be two types which is general personal data and sensitive personal data.⁵²

Firstly, general personal data is for example name and family name, address, email, an ID card number, location data, IP address, cookie ID, the advertising identifier of your phone or the data held by a hospital that could identifies a person.⁵³

Another type is sensitive personal data is specified in Article 9 of GDPR Processing of special categories of personal data of GDPR as follows:

“1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the

⁵¹ General Data Protection Regulation Article 4

⁵² intersoft consulting, ‘GDPR Personal data’ < <https://gdpr-info.eu/issues/personal-data/> > accessed 26 March 2023.

⁵³ European Commission, ‘What is personal data?’ <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> accessed 26 March 2023.

processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited..."⁵⁴.

The aforesaid types of data are used to apply in computing science for develop the machine learning.

2.6 Other Types of Personal Data

2.6.1 Sensitive Personal Data or Sensitive Data

Sensitive data ⁵⁵refers to any information that, if disclosed or accessed by unauthorized individuals, could lead to harm, privacy violations, or potential misuse. This data often includes personally identifiable information such as race, ethnicity, religious beliefs, sexual orientation, biometric data, and other sensitive details.

Protecting sensitive data is crucial to ensure privacy, maintain security, and comply with legal and ethical standards. Organizations and individuals must take appropriate measures to safeguard sensitive data from unauthorized access, breaches, or misuse. This includes implementing strong data encryption, access controls, secure storage, and regular security assessments.

Additionally, data protection regulations such as the General Data Protection Regulation (GDPR) Article 9⁵⁶ and the California Consumer Privacy Act (CCPA) Section 1798.100. (a) (2)⁵⁷, provide guidelines and legal requirements for handling sensitive data. These regulations aim to protect individuals' privacy rights and mandate organizations to handle sensitive data responsibly and securely.

Sensitive data is often referred to as "special categories of personal data" in the General Data Protection Regulation (GDPR). The GDPR gives special protection

⁵⁴ General Data Protection Regulation Article 9

⁵⁵ Abi Tyas Tunggal, 'What is Sensitive Data?' < <https://www.upguard.com/blog/sensitive-data> > accessed 20 June 2023.

⁵⁶ *supra note.*, 54

⁵⁷ California Consumer Privacy Act (CCPA)/ California Privacy Rights Act (CPRA) Section 1798.100. (a) (2)

to sensitive data, which means that organizations that process sensitive data must take additional measures to protect this data.

When handling sensitive data, it is important to follow best practices and security protocols to minimize the risk of data breaches and protect individuals' privacy. This includes practices such as data minimization (collecting and retaining only the necessary data), obtaining explicit consent for data collection and processing, and implementing proper data retention and disposal policies.

Overall, handling sensitive data requires diligence, adherence to security measures, and a commitment to privacy protection to ensure the confidentiality and integrity of the data and maintain the trust of individuals and organizations involved.

2.6.2 Anonymous Data

Anonymous data refers to information that has been processed or transformed in a way that it can no longer be directly linked to an individual or entity. It is data from which any personally identifiable information (PII) has been removed or sufficiently modified to prevent identification.

The purpose of anonymizing data is to protect privacy while still enabling analysis, research, or other activities that require working with large datasets. By removing or de-identifying PII, anonymous data aims to prevent the identification of specific individuals, reducing the risk of privacy breaches and unauthorized access.

However, it is important to note that the process of anonymization does not guarantee absolute anonymity. In certain cases, with sufficient resources and additional information, it may be possible to re-identify individuals from supposedly anonymized data. Therefore, data anonymization techniques should be carefully implemented and regularly assessed to maintain a balance between data utility and privacy protection.

Anonymous data is commonly used in research, statistical analysis, and data sharing initiatives. By sharing anonymized datasets, organizations can facilitate collaborative research, draw insights, and develop solutions while preserving privacy and complying with data protection regulations.

It is crucial to handle anonymous data responsibly, ensuring that the anonymization process is robust and that appropriate safeguards are in place to

prevent re-identification. By doing so, the benefits of working with large datasets can be realized while respecting individuals' privacy rights.

2.7 Big Data

The concept of big data refers to datasets that are characterized by their size, complexity, and velocity, making them challenging to process and analyze using traditional methods. The term gained significant attention in the early 2000s when industry analyst Doug Laney introduced the widely recognized definition of big data based on three key characteristics⁵⁸, known as the three V's:

a. Volume

Big data involves a massive volume of data⁵⁹, typically ranging from terabytes to petabytes and even exabytes. This includes vast amounts of structured, semi-structured, and unstructured data generated from various sources such as social media, sensors, transactions, and more.

b. Velocity

Big data is generated at high velocity, with data being produced and collected rapidly and continuously. This includes real-time or near-real-time data streams that require efficient processing to extract valuable insights and enable timely decision-making.

c. Variety

Big data encompasses a wide variety of data⁶⁰ types and formats. It includes structured data (e.g., databases and spreadsheets), unstructured data (e.g.,

⁵⁸ Sumeet Bansal, 'What Are the Key Characteristics of Big Data?' <<https://www.analytixlabs.co.in/blog/characteristics-of-big-data/>> accessed 20 June 2023.

⁵⁹ David Gewirtz, 'Volume, velocity, and variety: Understanding the three V's of big data' <<https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/>> accessed 20 June 2023.

⁶⁰ Marc Dimmick, 'How the Variety in Big Data Works as an Advantage' <<https://opengovasia.com/how-the-variety-in-big-data-works-as-an-advantage/>> accessed 20 June 2023.

text, images, videos), and semi-structured data (e.g., XML, JSON). The diversity of data sources and formats adds complexity to the processing and analysis tasks.

In addition to the three V's, other characteristics have been recognized as part of the big data paradigm, such as veracity (data quality and trustworthiness) and value (the potential insights and value that can be derived from analyzing the data).

To effectively handle big data, specialized technologies and approaches have emerged, including distributed computing frameworks like Apache Hadoop and Apache Spark, scalable storage systems, and advanced analytics techniques such as machine learning and data mining⁶¹. These tools enable organizations to store, process, analyze, and extract actionable insights from large and complex datasets, leading to improved decision-making, innovation, and efficiency in various fields.

2.8 Personal Data Protection

Data protection is indeed centered around safeguarding information pertaining to identified or identifiable individuals, encompassing a broad range of personal data such as names, dates of birth, photographs, video footage, email addresses, telephone numbers, IP addresses, and communication content.

The concept of data protection is closely linked to the right to privacy, as both play vital roles in upholding fundamental values, rights, and freedoms. Data protection regulations and privacy laws are in place to ensure that personal data is handled fairly, with respect to individuals' rights, and processed appropriately by both public and private entities.

Data protection regulations⁶², such as the General Data Protection Regulation (GDPR), outline specific aims to govern the collection, use, and storage of

⁶¹ Craig Stedman, 'data mining'

<<https://www.techtarget.com/searchbusinessanalytics/definition/data-mining> > accessed 20 June 2023.

⁶² Securiti Research Team, 'Data Privacy Laws and Regulations Around the World' <<https://securiti.ai/data-privacy-laws/> > accessed 20 June 2023.

personal data. These aims include promoting transparency, securing the lawful and fair processing of data, respecting individuals' rights to access and control their data, and establishing mechanisms for accountability and enforcement.

By adhering to data protection principles and regulations, organizations and individuals contribute to maintaining privacy, upholding fundamental rights, and facilitating the responsible use of personal data in both the public and private sectors.

2.9 Data Protection Principles

The principles of data protection⁶³ serve as foundational guidelines for ensuring the fair and lawful processing of personal data. These principles provide a framework for organizations and individuals to handle personal data responsibly and protect individuals' privacy rights. While specific regulations may vary, the following are common principles found in many data protection frameworks, such as the General Data Protection Regulation (GDPR)⁶⁴:

a. Fairness and Transparency

Personal data must be processed lawfully, with a legitimate basis for processing, and in a transparent manner that ensures individuals are aware of the purposes and processing activities involving their data.

b. Purpose Limitation

Personal data should be collected for specified, explicit, and legitimate purposes. It should not be further processed in a way incompatible with those purposes.

⁶³ European Union Agency for Fundamental Rights, Handbook on European data protection law 2018 Edition, p.115-137.

⁶⁴ European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, p.44-48.

c. Data Minimization

The collection of personal data should be limited to what is necessary for the intended purposes. Organizations should minimize the amount and extent of data collected, ensuring it is relevant and adequate for the purposes at hand.

d. Accuracy

Personal data should be accurate, kept up to date, and necessary steps should be taken to rectify or erase inaccurate or outdated information.

e. Storage Limitation

Personal data should be retained only for as long as necessary to fulfill the purposes for which it was collected, unless there is a legal obligation or other legitimate basis for longer retention.

These principles help guide the handling of personal data, promoting responsible data practices, privacy protection, and individuals' rights. Adhering to these principles ensures that personal data is processed fairly, securely, and in compliance with legal requirements.

2.10 Automated Decision-Making

Automated decision-making refers to the process of making decisions without any human involvement, where the decisions are made by automated systems or algorithms. These decisions can be based on factual data, as well as on digitally created profiles or inferred data⁶⁵.

Automated decision-making often relies on the analysis of large volumes of data using machine learning algorithms or artificial intelligence techniques. These algorithms can identify patterns, make predictions, or assess risks based on the

⁶⁵ European Commission, 'Can I be subject to automated individual decision-making, including profiling?' <https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_en> accessed 20 June 2023.

available data. The decisions made by automated systems can have significant implications for individuals, such as determining eligibility for a loan, job application screening, or personalized advertising.

Automated decision-making can be beneficial in terms of efficiency, scalability, and objectivity. However, it also raises concerns about transparency, fairness, and potential biases. The use of inferred data or digitally created profiles, which may not be directly provided by individuals, can introduce additional challenges and risks.

Data protection regulations, such as the General Data Protection Regulation (GDPR), recognize the potential impact of automated decision-making on individuals' rights and have specific provisions regarding such processing. These regulations often require organizations to provide individuals with information about the logic, significance, and consequences of automated decision-making and offer the right to challenge or seek human intervention in such decisions.

It is important for organizations to be transparent and accountable in their automated decision-making processes, ensuring that appropriate safeguards and mechanisms are in place to address potential risks and biases. Regular monitoring, auditing, and review of automated systems can help mitigate potential adverse effects and ensure compliance with legal and ethical standards.

2.11 Concerning of Personal Data Processing by Machine Learning

In this era, artificial intelligence is developed by several organizations. Especially, machine learning, which is the algorithm driving artificial intelligence inside, is trained by computer science to learn the special experience for improvement.

As mentioned, the developer needs to apply the information as an input in the algorithm to make it learn. If they put more, the progress also increases well definitely. For example, the diagnosis examination machine needs the information of several types of diagnosis to learn for making most accurate decision in the diagnosis examination, so the computer science, who try to develop this algorithm, need to

collect the data of several types of diagnosis and put on the machine learn to let the machine learn.

Presently, when you open application such as YouTube, you will see the channel that you frequently see throughout the last couple of months has appeared at the first or second clip in the screen, and YouTube will clarify your interested channel and show on your screen in the appropriated time. This will facilitate you to choose the favorite channel to watch for each time. How could YouTube do this outcome? The answer is machine learning.

Most of remarked tech company in the world apply the algorithm to work for convince the customer to use their application. Some are attempted to have their own algorithm and other choose to utilize the service of expertise company.

Whereas personal data is the key factor of training the algorithm or machine learning. The personal data is collected by each company as a big data in several such as in the photo stock vector website, search engine website or chat application. After that the big data would be service commercially for the tech company who are training the machine learning and, in some matter, the personal data will be put in algorithm without the consent of the personal data subject that cause the damages or conflict for the data subject so on.

For example, *Burke v. Clearview AI, Inc.*, Case No.: 3:20-cv-00370-BAS-MSB (S.D. Cal.)⁶⁶ (filed February 27, 2020) held in Southern District of California Court. The complaint alleges that Clearview's facial recognition technology which scrapes, without notice or consent, social media websites for images of consumers' faces violates, among other laws, both the California Consumer Privacy Act of 2018 (CCPA) and Illinois Biometric Information Privacy Act (BIPA) of 2008. According to the complaint, Clearview's facial recognition software uses the billions of scraped images in its database to generate a type of biometric information, known as a "faceprint," to match a face to other personally identifiable information; it then sells access to the faceprint database to law enforcement agencies and private companies. The complaint

⁶⁶ *Burke v. Clearview AI, Inc.*, Case No.: 3:20-cv-00370-BAS-MSB (S.D. Cal.)

charges that Clearview improperly collected personal information without properly notifying consumers.⁶⁷

Now, it is very convenient in breaching of the right of personal data protection of the data subject. The personal data should be used by consent of the data subject prior to the processing of the data. Especially, in Thailand have the Personal Data Protection Act B.E.2562 but that Act is appropriate for personal data breaching by algorithm or machine learning, or it need to add more regulation for this special case.



⁶⁷ Lee Johnston, 'Recent cases Highlight Growing Conflict Between AI and Data Privacy' <<https://www.haynesboone.com/news/publications/recent-cases-highlight-growing-conflict-between-ai-and-data-privacy>> accessed 1 April 2023.

CHAPTER 3

MEASURES OF PERSONAL DATA PROTECTION UNDER LAW

The thesis focuses on proposing appropriate measures for the protection of personal data in the processing of artificial intelligence under Thai law, with a specific focus on machine learning.

In this Chapter, to verify the appropriate measures, the author studies Thai law in comparison with foreign law. In terms of foreign law, the General Data Protection Regulation (GDPR), which is the model law for data protection in civil law countries, is the most influential law from the European Union.

On the one hand, common law countries have also enacted major data protection bills. In this regard, the California Consumer Privacy Act (CCPA), which was amended by the California Privacy Rights Act (CPRA), is in the spotlight as the first data protection bill in the United States that has inspired other states to draft their own data protection laws.

3.1 Personal Data Protection in the Kingdom of Thailand

The Constitution of the Kingdom of Thailand, as the supreme, always recognizes the fundamental right of Thai citizen such as right to privacy, human right, or human dignity etc., personal data protection is also one the right to privacy. Moreover, there are many laws in Thailand which is capable to apply to protect data subject form the infringement. Hence, this Chapter hereby considers such laws and its enforcement.

3.1.1 The Constitution of the Kingdom of Thailand

In the Constitution of the Kingdom of Thailand B.E. 2560, It is indeed important to recognize that the right to privacy, dignity, reputation, and family is

enshrined in Section 32⁶⁸ of the Constitution. This provision aims to protect the fundamental rights of individuals, including the protection of personal information.

According to Section 32 which is espoused that “Section 32. A person shall enjoy the rights of privacy, dignity, reputation and family.

An act violating or affecting the right of a person under paragraph one, or an 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.”⁶⁹.

Paragraph 1 of Section 32 means Thai person certain rights that encompass privacy, dignity, reputation, and family. The rights of privacy, dignity, reputation, and family are fundamental human rights that are protected by international law and the laws of many countries. These rights are important because they protect individuals from interference in their personal lives and ensure that they are treated with respect and dignity.

Then, in paragraph 2 prescribed that any act that violates or affects the right of a person, or exploits personal information, is not permitted unless it is authorized by law and is necessary for the public interest. This provision establishes the principle that personal information should not be used or exploited without a legal basis.

As mentioned in paragraph 2 “...an 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.”, Its means that the constitution forbids the use of personal information also known as personal.

The exception mentioned in paragraph 2 of Section 32 allows for the use of personal data when it is recognized by law. However, such laws must be enacted only to the extent necessary and for the benefit of the public which is Personal Data Protection Act B.E. 2562 effective in 2022. This emphasizes the

⁶⁸ Nakorn Serirak, Kwam Pen Suan Tua Pai Tai Rattathanmanoon Mai Tong Jap Ta [Right to Privacy under current the Constitution of Thailand] (นคร เสรีรักษ์, ‘ความเป็นส่วนตัวภายใต้รัฐธรรมนูญใหม่ “ต้องจับตา”’) < <https://ilaw.or.th/node/4255> > accessed 20 June 2023.

⁶⁹ The Constitution of the Kingdom of Thailand B.E. 2560 Section 32

importance of ensuring that any collection, use, or disclosure of personal information is done in accordance with legal requirements and for legitimate purposes.

By recognizing the right to privacy and imposing restrictions on the use of personal information, the Constitution of Thailand provides a foundation for the protection of individuals' privacy rights and personal data within the country.

In this regard, there are other four laws of Thailand which is the laws would govern as appropriate measure for personal data protection.

3.1.2 Civil and Commercial Code

In wrongful acts provision under Civil and Commercial Code or Thai CCC, Section 420 is espoused that “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 therefore.”⁷⁰

Section 420⁷¹ of the Civil and Commercial Code of Thailand (CCC) sets out the elements of a tortious act, which is an act that violates the rights of another person and causes them damage. The four elements of a tortious act under Section 420 are:

Unlawfulness: The act must be unlawful, which means that it must be a violation of a right that is protected by law.

Intention or Negligence: The act must be intentional or negligent. Intentional means that the person who committed the act knew that their actions were likely to cause harm and that they went ahead and did it anyway. Negligent means that the person who committed the act did not take reasonable care to avoid causing harm.

Damages: The act must cause damage to the other person. Damage can be physical, financial, emotional or entitlement.

⁷⁰ Civil and Commercial Code Section 420

⁷¹ Sanankorn Sotthibandhu, Kham Athibai Kod Mai Laksana La Merd Chat Kan Ngan Nok Sang Lea Lab Mi Kuan Dai [Explanations of Civil and Commercial Code oh Torts, Agency Without Specific Authorization Undue Enrichment] (3rd edition, Winyuchon, 2010) (ศนันท์ภรณ์ โสทธิพันธ์, คำอธิบายกฎหมายลักษณะละเมิดจัดการงานนอกสั่งละลามิควรได้ (พิมพ์ครั้งที่ 3, วิญญูชน 2553)), p.282

Causation: The damage must be caused by the act. This means that the act must be the direct or proximate cause of the damage.

If all four of these elements are present, then the person who committed the act will be liable to the other person for the damage that they caused. The amount of compensation that the person who committed the act will have to pay will depend on the extent of the damage that they caused.

The main principle of tort law is that people should be held responsible for the damage that they cause to others. This principle helps to protect people from harm and to ensure that those who are responsible for causing harm are held accountable.

The damages included “any right of another person”. When the right of personal data is recognized under Section 32 of the Constitution of Thailand, the provision, therefore, extends to personal data infringement also.

Because this Section is the basis of legal protection under Thai CCC for the person who have got any damages from others. Even if this Section is not focus sole on the data protection. If Thailand without the specific law regarding data protection, this Section could be applied to protect the individual from personal data infringement.

In Thai CCC, there is the Section 437 is espoused that “A person is responsible for injury caused by any conveyance propelled by mechanism which is in his possession or control, unless he proves that the injury results from force majeure or fault of the injured person.

The same applies to the person who has in his possession things dangerous by nature of destination or on account of their mechanical action.”⁷²

Section 437 of the Civil and Commercial Code of Thailand (Thai CCC) sets out the liability of a person who possesses or supervises a vehicle walking with mechanical power for damage caused by the vehicle. The Section states that the

⁷² Civil and Commercial Code Section 437

person will be liable for the damage unless they can prove that the damage was caused by force majeure or the fault of the victim.

Section 437 paragraph two of the Thai CCC extends this liability to persons who have in their possession property that is dangerous by its condition, intent to use, or mechanism. This means that a person who has a dangerous object in their possession and who fails to take reasonable care to prevent it from causing harm may be liable for any damage that is caused⁷³.

The liability under Section 437 of the Thai CCC is strict liability, which means that the person who is liable does not have to prove that they were negligent. This is because the law recognizes that vehicles and other dangerous objects can cause serious harm, and that it is in the public interest to hold the persons who have them in their possession responsible for the damage that they cause.

This Section is mostly construed to apply with the damages from automate vehicle or drone. This is because drones are considered to be vehicles walking with mechanical power, and they can cause serious harm if they are not operated safely.

Section 437 of Thai CCC states that a person who possesses or supervises a vehicle walking with mechanical power is responsible for the damage caused by the vehicle unless they can prove that the damage was caused by force majeure or the fault of the victim.

The autopilot system of an automated vehicle is a part of the vehicle, so it is possible that Section 437 could apply to damage caused by an automated vehicle while driving with an autopilot system. However, there are some factors that could affect whether the person who possesses or supervises the vehicle would be held liable for damage caused by an automated vehicle.

⁷³ Bhumindr Butr-Indr, Law and Artificial Intelligence (AI), Thammasat Law Journal, Vol.47 No.3 (September 2018) (ภุมินทร บุตรอินทร์, กฎหมายกับปัญญาประดิษฐ์, วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, ปีที่ 47 ฉบับที่ 3 (กันยายน 2561)), p.507.

3.1.3 Official Information Act B.E. 2540

In this part, the author considering on the Official Information Act B.E. 2540 in Thailand⁷⁴, this Act emphasizes the right of Thai people to participate in the government of the country and access official information. It also includes provisions related to personal data protection.

Section 4⁷⁵ of the Act defines personal information as information related to personal particulars of a person, such as education, financial status, health record, criminal record, or employment record, which contains the person's name or identifying elements like fingerprints, recordings, photographs, and more. It also includes information about deceased individuals.

The Act primarily focuses on the right to know and access individual or public information held by government organizations in a legitimate manner. Section 9 specifies the official information that state agencies must make available for public inspection, subject to Section 14 and Section 15⁷⁶. This includes decisions affecting private individuals, policies or interpretations, work plans, manuals or orders affecting private individuals' rights and duties, published materials, concession contracts, resolutions of the Council of Ministers, and other information determined by the Board. If any part of the information is prohibited from disclosure, it must be appropriately handled to protect such information.

Any person, regardless of their interest in the matter, has the right to inspect, obtain a copy, or obtain a certified copy of the official information mentioned in Section 9. State agencies may establish rules on the collection of fees, considering concessions for individuals with low incomes, with approval from the Board. The extent to which an alien can enjoy these rights is determined by the Ministerial Regulation.

Government organizations are obligated to comply with Section 9⁷⁷ and provide at least the specified official information for public access. The Information

⁷⁴ Official Information Act B.E. 2540

⁷⁵ Official Information Act B.E. 2540 Section 4

⁷⁶ Official Information Act B.E. 2540 Section 14-15

⁷⁷ Official Information Act B.E. 2540 Section 9

Committee regulates these duties, which may include providing accessible places for people to access information, providing detailed indexes or lists, and more.

Additionally, the Act allows individuals to duplicate official information with certification for organizational purposes. Section 11 addresses requests for specific official information that has not been published or made available for public inspection. Responsible state agencies must provide the requested information within a reasonable period, unless the request is excessive or made frequently without reasonable cause. The agency may request an extension if the information is easily damaged or provide copies in a suitable condition to avoid damage. The provisions of Section 9 relating to fees, provision of information, and creating new official information apply *mutatis mutandis* to the provision of information under Section 11⁷⁸.

In summary, the Official Information Act B.E. 2540 in Thailand ensures the right of Thai people to participate in the government and access official information. It outlines the responsibilities of government agencies in providing information, and individuals have the right to request and obtain specific official information, subject to certain conditions and reasonable timeframes.

3.1.4 Electronic Transactions Act B.E. 2544

The Electronic Transactions Act B.E. 2544 (ETA)⁷⁹ is a Thai law that regulates electronic transactions. The ETA was enacted in 2544, and it was the first law in Thailand to specifically address electronic transactions.

This legislation defines an electronic transaction as "any transaction in which information is transmitted, stored, or processed electronically." This includes transactions that are conducted through electronic mail, websites, and other electronic means.

Such act provides for the legal recognition of electronic transactions. This means that electronic transactions are given the same legal effect as paper-based

⁷⁸ Official Information Act B.E. 2540 Section 11

⁷⁹ Electronic Transactions Act B.E. 2544

transactions. For example, an electronic contract is just as valid as a paper-based contract.

This provision acknowledges the legal recognition of contracts formed through automated electronic systems and ensures that they are treated as valid and enforceable under Thai law.

Section 4⁸⁰ is espoused that “automated electronic message system” means a computer program or an electronic means or other automated means used to initiate an action or respond to data messages or any performances against data messages in whole or in part, without review or intervention by a natural person each time an action is initiated or each time a response is generated by the system”

This means that an automated electronic message system is a computer program or other automated means that is used to send or receive electronic messages without the need for human intervention. For example, an automated electronic message system could be used to send emails or to process online transactions.

This Section was added in the third amendment of EAT which was enacted in 2019 for dealing with the AI in any transactions.

a. Right to Obtain Human Intervention

Section 13/2⁸¹ is espoused that “A contract formed by the interaction of an automated electronic message system and a natural person, or of automated electronic message systems, shall not be denied validity or enforceability on the sole ground that no natural person intervened in each of the individual actions carried out by the automated electronic message systems or the resulting contract.”

This Section emphasizes that contracts formed through interactions between automated electronic message systems and natural persons, or between automated electronic message systems themselves, should not be invalidated or considered unenforceable solely because there was no direct involvement of a natural

⁸⁰ The Electronic Transactions Act B.E. 2544 Section 4.

⁸¹ The Electronic Transactions Act B.E. 2544 Section 13/2.

person in each individual action or step taken by the automated systems. In other words, the absence of human intervention in the formation of the contract does not render it invalid or unenforceable.

This provision acknowledges the increasing use of automated systems in contract formation and recognizes their legal validity. It implies that contracts entered into through automated means can still be binding and enforceable, even if they do not involve direct human intervention in each specific action or decision made during the process.

This Section merely is the exception of right to obtain human intervention because the absence of human intervention in the formation of the contract does not render it invalid or unenforceable. Additionally, this Section focusses on defining the transaction between human and automated electronic message systems, not recognize the right to the data subject.

b. Right to Rectification or Right to Correct

Section 17/1⁸² is espoused that “In the case where an input error is made by a natural person and sent through an automated electronic message system of another party and such automated electronic message system does not provide the person with a channel for correcting the resulting error, such person or the representing party has the right to withdraw the portion of the declaration of an intention in which the input error occurred if:

(1) such person or the representing party forthwith notifies the other party of the error after having learned of such error and satisfies that the error has been made through the automated electronic message system; and

(2) such person or the representing party has not materially used or received any benefit from the goods or services or any other thing from the other party.”

This Section is important because it protects people from making unintentional mistakes when using automated electronic message systems. For example, a person might accidentally enter the wrong price for a product when making

⁸² The Electronic Transactions Act B.E. 2544 Section 17/1

an online purchase. If the automated electronic message system does not allow the person to correct the error, then the person would be bound by the mistaken price. Section 17/1 of the ETA allows the person to withdraw the declaration of intention and avoid being bound by the mistaken price.

This Section recognized the “Right to Rectification or Right to Correct”. In contrary, this Section is prescribing the incorrection by natural person not from the data controller. Section 17/1 is not focus on personal data protection.

c. Right to Be Informed

Section 19⁸³ . is espoused that “In the case where an acknowledgement of receipt of a data message is required, whether at the originator’s request or as agreed with the addressee before or at the time of sending the data message or by means of that data message, the following rules shall apply:

(1) in the case where it has not been agreed by the originator that the acknowledgement be given in a particular form or by a particular method, the acknowledgement may be given by any communication by the addressee, whether by an automated information system or by any other method, or by any conduct of the addressee sufficient to indicate to the originator that the addressee has received the data message;

(2) in the case where the originator has stated a condition that the data message shall be regarded as having been sent only upon receipt of an acknowledgement by the addressee, it shall be deemed that the data message has never been sent until the originator has received the acknowledgement;”

Section 19 of the Electronic Transactions Act B.E. 2544 (ETA) sets out the requirements for acknowledgement of receipt of a data message. The Section states that an acknowledgement of receipt is required if it is requested by the originator or if it is agreed upon by the originator and the addressee.

The Section also states that an acknowledgement of receipt must be sent within a reasonable time after the data message is received. The Section does not specify what constitutes a reasonable time.

⁸³ The Electronic Transactions Act B.E. 2544 Section 19

In Summary, the Electronic Transactions Act (ETA) of Thailand does recognize the Right to Obtain Human Intervention, Right to Rectification or Right to Correct, and Right to be informed. However, these rights are only related to the electronic transaction itself and do not cover all aspects of personal data protection.

The most relevant law for personal data protection in Thailand is the Personal Data Protection Act B.E.2562 (PDPA). The PDPA provides a comprehensive framework for the protection of personal data in Thailand. It includes provisions on the collection, use, and disclosure of personal data, as well as the rights of individuals with respect to their personal data.

3.1.5 Personal Data Protection Act B.E.2562

Thailand already accepted the theory of data protection from GDPR of European Union to apply in Thailand in Personal Data Protection Act, B.E. 2562⁸⁴

In the act provide the right to know of person who want to know his information that what use by the data collection entity. This provision is transparency that can apply over artificial intelligence

In the law, the right is defined transparency policy which is exercising by committee, data owner and data controller.

3.1.5.1 Personal Data Protection Principles under Personal Data Protection Act B.E. 2562

In this Chapter, the author would consider on the personal data protection principle set forth in Personal Data Protection Act B.E. 2562. There are the provisions is stipulated to recognize the principle to protect the data subject as follows:

a. Fairness and Transparency

The Personal Data Protection Act (PDPA) of Thailand incorporates principles of fairness and transparency in multiple Sections, such as Section 23, Section 24, and Section 26. However, it is essential to note that these principles are not explicitly tied to data processing activities in the PDPA.

⁸⁴ Personal Data Protection Act, B.E. 2562

b. Purpose Limitation

The purpose limitation principle espoused in Section 21⁸⁵ of PDPA which provide the duty of the data controller to collect, use, or disclose the personal data compliance with the prior purpose which notify to the data subject.

The data controller shall not use such data different from the prior purpose unless the data controller already informs the new purpose to the data subject and then accept the consent legitimately from the data subject before such use, or there is any legal provision grant the data controller to proceed.

c. Data Minimisation

Section 22 of the PDPA in Thailand⁸⁶ emphasizes the data minimization principle, which ensures that personal data is collected in a manner that is limited to what is necessary for the lawful purpose of the data controller. This helps safeguard the privacy of data subjects by preventing unnecessary or excessive collection of their personal information.

d. Accuracy

The accuracy of the personal data is significant of the data processing because the wrong data cause the error output precisely. In Section 35⁸⁷ of PDPA states the duty of data controller to maintain the accuracy of the personal data to protect the misleading for the personal data, in addition the personal data shall be in up-to-date and completion condition.

e. Storage Limitation

According to Section 37⁸⁸ third paragraph, the Data Controller has a duty to put in place an examination system to determine the erasure or destruction of Personal Data in the following situations:

1. When the retention period specified for the Personal Data ends.

⁸⁵ Personal Data Protection Act, B.E. 2562 Section 21

⁸⁶ Personal Data Protection Act, B.E. 2562 Section 22

⁸⁷ Personal Data Protection Act, B.E. 2562 Section 35

⁸⁸ Personal Data Protection Act, B.E. 2562 Section 37

2. When the Personal Data becomes irrelevant or is no longer necessary for the purpose for which it was collected.

3. Data Subject's Requests:

4. If the data subject withdraws their consent for the processing of their Personal Data.

3.1.5.2 Data Subject Rights under Personal Data Protection Act B.E.

2562

The Right of Data Subject recognizes in this Act in Chapter 1 and 2. In this part, the author will focus on the principle in such act as follows:

a. Right to Be Informed

The right to be informed is recognized in Section 23⁸⁹ of PDPA. Under such Section, the data subject shall be informed by the data collector regarding the specific matter stipulates in second paragraph in sub-Section (1) to (6) which consist of the specific matter as follows:

(1) The data subject shall be informed regarding the purpose of collection.

(2) The data subject shall be informed the duty to deliver the personal data subject under legal base or agreement base including the possible effect of reject this duty.

(3) The data subject shall be informed the data type would be collected including the period of collection

(4) The data subject shall be informed regarding the third person or organization that might receive such personal data to.

(5) The data subject shall be informed the information of data collection and data protection such as any contact, any representative.

(6) The data subject shall be informed the right of data subject under PDPA

b. Right to Access

⁸⁹ Personal Data Protection Act, B.E. 2562 Section 23

The right to access is stipulated in Section 30 and 31 in which the data subject is able to access or duplicate the personal data under the responsibility of data controller.

Moreover, the data subject is able to request the disclosure of the personal data acquired without legitimated consent also.

The duty of the data controller set forth in this Section is to accept the data subject's request and to provide the information within thirty days.

The exception to reject the request of the data subject is stated in second and third paragraphs. The right to reject of the data controller recognizes under Section 30⁹⁰ which consist of legal permission or court order base, and the damages of the public interest base.

c. Right to Data Portability

The data subject entitles to request the data controller to provide the personal data in which such personal data is in the electronic form subject to Section 31⁹¹. In addition, the data subject also have the right to request the data controller to transfer the personal data in electronic form to the other data controller and to request the other data controller to proceed such transfer directly.

This Section also recognizes the exemption to reject the request of the data subject in third paragraph which states that when the transfer of the personal data is proceed subject to the public interest, or law the data controller entitles to reject that request.

d. Right to Object

PDPA also recognizes the right to object in Section 32⁹². In PDPA, the data subject is able to oppose the collection, use, or disclose his/her own data whenever legally.

This Section states the type of personal data which the data subject entitles to object as follows:

⁹⁰ Personal Data Protection Act, B.E. 2562 Section 30

⁹¹ Personal Data Protection Act, B.E. 2562 Section 31

⁹² Personal Data Protection Act, B.E. 2562 Section 32

(1) The personal data which under the exemption to consent subject to Section 24 (4) or (5), unless

(a) The data controller demonstrates that there is a compelling legitimate ground.

(b) The personal data is carried out for the establishment, compliance or exercise of legal claims, or defense of legal claims.

(2) The personal data for the purpose of direct market.

(3) The personal data for the purpose of scientific, historical or statistic research

In this matter. If the data subject entitles the right to object, the data controller shall suspend the collection, use, or disclose such personal data forward, and divide into the personal data from other data.

e. Right to Erasure

The right to erasure is recognized in Section 33⁹³. The data subject entitles to request the erasure of personal data or anonymize the personal data to become the anonymous data which in the condition as follows:

(1) Unnecessary for collection, use, or disclose by the purpose of the first consent.

(2) The data subject withdraws the consent and the data controller collect such data without legitimate ground.

(3) The data subject entitles the right to object under Section 32 without any exemption.

(4) The personal data is collected illegally.

However, the personal data is collected by the purpose under Section 24(1) or (4) or Section 26 (5)(a) or (b) or the purpose from legal basis could not be erased.

If the request to erase cause any expenses, such expense shall be on the data controller responsibility.

⁹³ Personal Data Protection Act, B.E. 2562 Section 33

In addition, the data subject entitles to complain the data controller who does not comply with the request with the committee.

f. Right to Restrict Processing

The data subject has the right to restrict processing under PDPA. Such right set forth in Section 34⁹⁴. It this Section classify the condition of personal data that could be restricted the processing such as.

(1) The personal data is in the examination for remains accurate, up-to-date, complete, and not misleading.

(2) The personal data shall be deleted because the illegal purpose, but the data subject decide to restrict.

(3) The personal data is unnecessary to retain complying with the purpose, however the data subject request to retain in order to the legal purpose.

(4) The personal data is under the request to object by the data subject then the data controller contest the request to verify that such personal data is collected, used, or disclosed by the legal base or public interest.

If the data controller does not comply with the request to restrict processing, the data subject have a right to complain to the committee.

g. Right to Rectification

The right to rectification is recognized in Section 35 and Section 36 of PDPA⁹⁵. In Section 35 states the duty of the data controller to remain the accurate, up-to-date, complete, and not misleading of the personal data. On the other hand, the data subject also has a right to examine the accurate, up-to-date, complete, and not misleading of his/her own personal data by requesting the data controller to examine such personal data which stipulates in Section 36.

h. Right to Withdraw Consent

The consent is the fundamental right of the data subject relating the personal data protection. On the other hand, to withdraw the consent

⁹⁴ Personal Data Protection Act, B.E. 2562 Section 34

⁹⁵ Personal Data Protection Act, B.E. 2562 Section 35-36

shall be recognized as well. In Section 19⁹⁶ fifth and sixth paragraphs of PDPA states such right to protect the data subject interest.

Subject to Section 19, the data subject entitles to withdraw the consent anytime which shall be proceeded easily. However, the withdrawal shall not affect the collection, use, or disclosure under the given consent. In addition, the data controller has a duty to inform the data subject regarding the affection of the withdrawal.

Event though, the right to withdraw consent could be used anytime, the right is limited subject to the legal basis or the contractual basis which give beneficial to the data subject.

3.2 Personal Data Protection in Foreign Law

The author will study the regimes regarding personal data protection governing in two alternative jurisdictions. The chosen countries are in the spotlight for their personal data protection regimes and for artificial intelligence, namely the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA).

3.2.1 General Data Protection Regulation (GDPR) of European Union (EU)

The European Union (EU) has introduced new laws to protect personal information. The law, known as "General Data Protection Regulation⁹⁷" or simply "GDPR", took effect on Friday 25 May 2018.

The law has changed the agreements of various companies. To store, record and process large volumes of data from EU populations, it is required to disclose what information the company will collect. And will they use the information next to anyone?

⁹⁶ Personal Data Protection Act, B.E. 2562 Section 19

⁹⁷ General Data Protection Regulation

This law will be in effect in 28 countries: Greece, Croatia, Czechia, Cyprus, Denmark, Netherlands, Bulgaria, Belgium, Portugal, Poland, France, Finland, Malta, Germany, Romania, Luxembourg, Luxembourg. Latvia, Lithuania, Spain, Slovakia, Slovenia, Sweden, the United Kingdom (Also known as England), Austria, Italy, Estonia, Ireland, and Hungary, all of which are members of the EU.

This law does not apply to IT companies only. But it also affects healthcare providers, insurers, banks, and many other companies inevitably dealing with sensitive personal information.

This means that EU-based companies (including the UK or the UK currently in the EU) have a digital presence. There are two options: obey the law. Or choose to receive a penalty that has a very high fine only

The deadline for adoption of the law is May 25, 2018, after the law was passed by the EU parliament.

Privacy observers pointed out that the Cambridge Analytica issue with Facebook emerged in March. This has made Internet users realizing why there is a need for GDPR laws that people have more control over their access to personal information from others.

GDPR is a big impact on how we collect data that will become digital footprint in the future, and it also has an impact on how we protect our data from service providers and apps.

Also, GDPR was stipulated to govern the automate decision making. There are the principals to access the core of decision making such as right to inform, right to access etc. the rule was stipulate in the difference categories of the law Now the author will state the information of the transparency in automate decision making in GDPR as follows:

3.2.1.1 Definition of Data Processing by Automated Means

In Article 4 (2)⁹⁸ of GDPR the definition of processing is stipulated “‘processing’ means any operation or set of operations which is performed

⁹⁸ General Data Protection Regulation Article 4(2)

on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

The definition of processing in the GDPR is broad and covers a wide range of activities. It includes any operation or set of operations that is performed on personal data, whether or not by automated means. This means that organizations must comply with the GDPR when they collect, store, use, or otherwise process personal data.

The GDPR also includes some specific requirements for certain types of processing activities. For example, the GDPR requires organizations to obtain consent from individuals before they can process their personal data for marketing purposes.

By understanding the definition of processing in the GDPR, organizations can ensure that they are complying with the law when they collect, store, use, or otherwise process personal data.

3.2.1.2 Data Protection Principles

a. Fairness and Transparency

Article 5⁹⁹ of the General Data Protection Regulation (GDPR) outlines the principles relating to the processing of personal data. It lays down the fundamental elements that data controllers and processors must adhere to when handling personal data. Among these principles are fairness and transparency, which are essential in ensuring that individuals' privacy rights are respected and protected throughout the data processing lifecycle.

b. Purpose Limitation

Article 5 of the General Data Protection Regulation (GDPR) sets out the fundamental principles relating to the processing of personal data. One of these key principles is purpose limitation, which is enshrined in Article 5(1)(b) of the GDPR. The purpose limitation principle emphasizes the necessity of specifying the

⁹⁹ General Data Protection Regulation Article 5

purposes for which personal data is collected and processed, ensuring that data is not used in a manner incompatible with those purposes¹⁰⁰.

c. Data Minimisation

The principle of data minimisation requires that data controllers only collect the personal data that is necessary for the specific purpose for which it is being collected. This means that data controllers should not collect more personal data than they need.

There are several ways in which data controllers can comply with the principle of data minimization

d. Accuracy

The principle of accuracy requires that data controllers ensure that the personal data they process is accurate. This means that data controllers should take steps to ensure that the personal data is up-to-date and that any inaccuracies are corrected as soon as possible.

The principle of accuracy is important because it helps to protect the rights of individuals. By ensuring that personal data is accurate, data controllers can help to ensure that individuals are not harmed by inaccurate information about them.

c. Storage Limitation

Article 5 of the General Data Protection Regulation (GDPR) outlines the fundamental principles that govern the processing of personal data. One of these key principles is storage limitation, which is established in Article 5(1)(e) of the GDPR. The storage limitation principle emphasizes the need for data controllers to retain personal data only for as long as is necessary for the purposes for which it was collected¹⁰¹.

3.2.1.3 Data Subject Rights

a. Right to Access

¹⁰⁰ *ibid.*

¹⁰¹ *ibid.*

GDPR grants individuals the right to request a copy of their personal data that is being processed by controllers, along with other relevant information. These requests are commonly known as "data subject access requests" or "access requests".

The right to access personal data is outlined in Article 15 of the GDPR. Additionally, in Article 15(h)¹⁰², it specifically addresses automated decision-making. According to this provision, individuals have the right to receive confirmation from the controller as to whether or not their personal data is being processed through automated decision-making, including profiling. If such processing is taking place, the individual has the right to access the personal data being used for this purpose. Furthermore, they are entitled to receive meaningful information about the logic involved in the automated decision-making process, as well as the significance and expected consequences of such processing for the data subject.

b. Right to Object to Processing of Personal Data

Under Article 21¹⁰³, data subjects have the right to object to the processing of their personal data when it is carried out in connection with tasks in the public interest, under official authority, or based on the legitimate interests of others. However, data subjects have a stronger right to object when the processing of their personal data is for direct marketing purposes. If a data controller is using personal data for direct marketing or profiling for direct marketing, data subjects can object at any time, and the data controller must cease processing the data upon receiving the objection. Data subjects can also object to the processing of their personal data for research purposes, except when it is necessary for tasks carried out in the public interest.

To exercise the right to object, data subjects must contact the data controller and provide grounds for their objection that relate to their particular situation. If the objection is valid, the data controller must stop processing the personal

¹⁰² General Data Protection Regulation Article 15(h)

¹⁰³ General Data Protection Regulation Article 21

data, unless they can demonstrate compelling legitimate reasons to continue processing. Data controllers can continue processing personal data if it is necessary for certain types of legal claims.

Data controllers are required to inform data subjects about their right to object at the time of the first communication, and if processing is conducted online, they must provide an online method for data subjects to exercise this right.

Under Article 22, data subjects have the right not to be subject to decisions based solely on automated processing that produce legal effects or significantly affect them. Automated processing is only permitted with the data subject's explicit consent, when necessary for the performance of a contract, or when authorized by Union or Member State law. Safeguards must be in place to protect the data subject's rights, freedoms, and legitimate interests. This may include the right to obtain human intervention, the right to present their point of view, and the right to challenge the decision. For special categories of personal data, processing is only lawful when the data subject has given explicit consent or when it is necessary for reasons of substantial public interest.

These rights are designed to give data subjects control over the processing of their personal data and to ensure that automated decisions do not have negative or unfair consequences for them.

c. Right to Erasure

The right to erasure, also known as the right to be forgotten, is one of the fundamental rights granted to individuals under the General Data Protection Regulation (GDPR). It is outlined in Article 17¹⁰⁴ of the GDPR and empowers data subjects to request the deletion or removal of their personal data from the control of data controllers under certain circumstances.

The right to erasure is a crucial aspect of data protection, providing individuals with control over their personal information and enabling them

¹⁰⁴ General Data Protection Regulation Article 17

to manage their online presence. By granting data subjects the right to have their data erased, the GDPR aims to ensure that individuals can exercise greater control over their personal information and have their privacy rights respected by organizations that process their data. Failure to comply with the right to erasure can lead to significant penalties and fines under the GDPR.

d. Right to Data Portability

The right to data portability is one of the fundamental rights enshrined in the General Data Protection Regulation (GDPR). It is established in Article 20¹⁰⁵ of the GDPR and grants data subjects the right to receive a copy of their personal data in a structured, commonly used, and machine-readable format. The purpose of this right is to empower individuals to move, copy, or transfer their personal data between different data controllers or service providers easily and without hindrance.

The right to data portability aims to promote data autonomy and empower data subjects to have more control over their personal information. By facilitating the transfer of personal data between different controllers, the GDPR seeks to enhance competition, innovation, and user choice in the digital environment while safeguarding individuals' privacy rights. Non-compliance with the right to data portability can lead to penalties and fines under the GDPR.

e. Right to Objecting to Profiling for Marketing

The right to object to profiling for marketing purposes is one of the fundamental rights under the General Data Protection Regulation (GDPR). It allows individuals to object to their personal data being used for profiling purposes in order to make marketing decisions about them.

Profiling is the process of using personal data to make predictions about individuals, such as their interests or behavior. In the context of marketing, profiling can be used to target individuals with specific marketing messages or to make decisions about whether to offer individuals certain products or services.

¹⁰⁵ General Data Protection Regulation Article 20

The right to object to profiling for marketing purposes is set out in Article 21(2) of the GDPR. The right to object to profiling for marketing purposes is an important right that allows individuals to control how their personal data is used. By exercising this right, individuals can protect their privacy and ensure that their personal data is not used for purposes that they do not consent to.

To exercise their right to object to profiling for marketing purposes, individuals can contact the data controller and request that their data be deleted or that it no longer be used for profiling purposes. The data controller must comply with the request within a reasonable period.

f. Right to Objecting to Processing for Research

The right to object to processing for research is one of the fundamental rights under the General Data Protection Regulation (GDPR). It allows individuals to object to their personal data being used for research purposes.

The right to object to processing for research is set out in Article 21(1) of the GDPR

The right to object is an essential component of data subjects' control over their personal data. By providing individuals with the right to object to processing for research purposes, the GDPR seeks to strike a balance between promoting scientific and historical research while ensuring data subjects' privacy rights are respected and protected. Data controllers must handle objections in a fair and transparent manner, taking into account the specific circumstances and the balance of interests between research purposes and individual rights. Failure to comply with the right to object may lead to penalties and fines under the GDPR.

3.2.1.4 Right to Information Specific on Automated Means

The processing of personal data should always be carried out in a lawful, fair, and transparent manner. Individuals should be clearly informed and aware that their personal data is being collected, used, consulted, or processed, and to what extent such processing occurs. The right to be informed, as outlined in Articles 13 and 14¹⁰⁶ of the GDPR, is crucial for organizations to ensure transparency.

¹⁰⁶ General Data Protection Regulation Article 13-14

Transparency requires that any information or communication related to the processing of personal data should be easily accessible, understandable, and presented in clear and plain language. This applies to information addressed to the public or the data subject and may include the use of visual aids when appropriate. When processing personal data of children, it is important to use language that is clear and easy for them to understand, as children require specific protection.

Individuals should be informed about the risks, rules, safeguards, and rights associated with the processing of their personal data, as well as how to exercise their rights in relation to such processing. The specific purposes for which personal data are processed should be explicit, legitimate, and determined at the time of data collection.

Under Article 13 of the GDPR, in addition to the information mentioned in paragraph 1, the controller is required to provide further information to ensure fair and transparent processing at the time of data collection. This includes disclosing the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4), and providing meaningful information about the logic involved, as well as the significance and expected consequences of such processing for the data subject.

Similarly, under Article 14, the controller must provide the data subject with additional information to ensure fair and transparent processing. This includes informing the data subject about the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4), and providing meaningful information about the logic involved, as well as the significance and expected consequences of such processing for the data subject.

3.2.1.5 Right to Explanation Specific on Automated Means

Under Article 22¹⁰⁷, individuals have the right not to be subject to a decision based solely on automated processing if it produces legal effects or significantly affects them. Automated processing refers to processing that is carried out without human intervention.

¹⁰⁷ General Data Protection Regulation Article 22

Automated processing is generally prohibited unless one of the following conditions is met:

The data subject has given their explicit consent to the automated processing, The automated processing is necessary for the performance of a contract between the data subject and the data controller, or the automated processing is authorized by Union or Member State law.

When one of these exceptions applies, suitable measures must be implemented to safeguard the rights, freedoms, and legitimate interests of the data subject. These measures may include providing the data subject with the right to obtain human intervention on the part of the data controller, the right to express their point of view, and the right to contest the decision.

Regarding machine learning processing that involves special categories of personal data, such processing can only be considered legitimate if the data subject has given explicit consent to the processing or if it is necessary for reasons of substantial public interest. Special categories of personal data include sensitive information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, and data concerning a person's sex life or sexual orientation.

The GDPR aims to ensure that individuals are not subjected to unfair or harmful decisions based solely on automated processing, and it provides them with specific rights and protections in these cases.

Recital 71¹⁰⁸ of the GDPR emphasizes the importance of suitable safeguards for automated processing. It states that individuals should have the right to be informed about the automated processing, including the logic involved and the significance and consequences of such processing.

Furthermore, individuals should have the right to obtain human intervention in the decision-making process, to express their point of view, to receive an explanation of the decision reached through automated processing, and to

¹⁰⁸ General Data Protection Regulation Recital 71

challenge the decision. These rights aim to ensure transparency, accountability, and fairness in automated decision-making that may significantly affect individuals.

Many experts argue that the reason the right to explanation was relegated to the Recitals is because the lawmakers did not intend to explicitly recognize its existence in the provisions. However, the author believes that this interpretation is exaggerated. There is a distinction between providing meaningful information about the rationale behind a decision, as outlined in Articles 13-15, including individual explanations as described in Recital 71. However, this difference may not be as significant as it appears.

In certain cases, it may be challenging for machine learning systems to provide a clear explanation of how an individual decision was made. This means that the requirements suggested in the provisions are more of a difference in degree rather than a distinct kind.

GDPR emphasizes the importance of providing meaningful information and explanation to individuals regarding automated decision-making, it does not explicitly mandate an extremely high level of transparency or a detailed explanation for each individual decision made by machine learning systems.

The regulation does require that individuals have sufficient insight into the logic and significance of the processing, enabling them to make informed decisions and exercise their rights. This means that individuals should have a general understanding of how their personal data is being processed by machine learning systems and the potential consequences or impacts of such processing.

Recital 71 of the GDPR specifically mentions the right to obtain an explanation of the decision reached after an assessment. This implies that individuals should have the ability to seek clarification or justification for decisions that significantly affect them and have an explanation provided in response.

a. Specific Information

Every processing should subject to safeguard measure to provide specific and meaningful information to the data subject empowers individuals to understand and contest automated decisions that may affect them.

b. Right to Obtain Human Intervention

The right to obtain human intervention is closely related to the right to explanation in the context of automated decision-making under the General Data Protection Regulation (GDPR). It is established in Article 22(3) of the GDPR and provides an additional layer of protection for data subjects when automated processing, including profiling, significantly affects them.

The right to obtain human intervention is an essential component of data protection, especially in the context of automated decision-making, as it ensures that human judgment is involved when decisions significantly affect individuals' rights and freedoms. By providing data subjects with the opportunity to express their point of view and contest automated decisions, the GDPR seeks to safeguard against potential biases or errors in automated processes and uphold individuals' rights to a fair and transparent decision-making process. Data controllers must be prepared to provide human intervention when requested by data subjects and adhere to the principles of fairness and accountability in their automated decision-making practices.

c. Right to Express Point of View

The right to express a point of view is an essential aspect of the right to obtain human intervention, which is established in Article 22(3) of the General Data Protection Regulation (GDPR). This right allows data subjects to have their say and provide additional information when automated decision-making, including profiling, significantly affects them.

The right to human intervention and the right to express a point of view are not absolute. Human intervention is not required if the automated decision-making is necessary for entering into or performing a contract, authorized by Union or Member State law, or based on explicit consent. However, even in these cases, data subjects still have the right to obtain an explanation of the decision and challenge the decision if they find it necessary.

The right to express a point of view is crucial in ensuring fairness and transparency in automated decision-making processes that significantly impact data subjects. By allowing individuals to provide input and additional information, the GDPR aims to minimize potential biases and errors in automated

decisions and promote a human-centric approach to decision-making when it significantly affects individuals' rights and freedoms. Data controllers must be prepared to address data subjects' point of view, consider their perspectives, and ensure that the decision-making process adheres to the principles of fairness, accountability, and respect for individuals' rights under the GDPR.

d. Right to Obtain an Explanation

The right to obtain an explanation is one of the fundamental rights under the General Data Protection Regulation (GDPR). It allows individuals to request an explanation from a data controller about the logic behind the processing of their personal data, as well as the significance and the envisaged consequences of such processing for the data subject.

The right to obtain an explanation is set out in Article 22(1) of the GDPR. The right to obtain an explanation empowers individuals to understand and challenge automated decisions that significantly affect them. By providing meaningful explanations, data controllers foster transparency, accountability, and fairness in automated decision-making processes. Data subjects have the opportunity to assess the validity and potential biases of these decisions and take appropriate actions if necessary. Data controllers must be prepared to provide clear explanations and ensure that individuals' rights to meaningful information and transparency are respected under the GDPR.

e. Right to Challenge the Decision

Under the General Data Protection Regulation (GDPR), data subjects have the right to challenge automated decisions that significantly affect them. This right is closely linked to the right to obtain an explanation and the right to human intervention, as established in Article 22 of the GDPR.

The right to challenge the decision is a crucial safeguard for data subjects to ensure that their rights and freedoms are protected in the context of automated decision-making. It enables individuals to contest automated decisions that they believe are biased, inaccurate, or based on incorrect data. By providing data subjects with the right to human intervention and the ability to express their point of view, the GDPR aims to uphold principles of fairness, accountability, and respect for

individuals' rights. Data controllers must be prepared to address challenges to automated decisions and conduct thorough reviews to ensure that decisions comply with the GDPR's requirements and protect individuals' rights.

3.2.1.6 Automate Decision-Making or Automated Processing Provision

Article 22 of the General Data Protection Regulation (GDPR) addresses automated decision-making, including profiling, and provides specific provisions regarding the prohibition, exceptions, safeguard measures, and the use of sensitive data in such processes.

1. Prohibition of Automated Decision-Making (Article 22(1)):

Article 22(1) GDPR establishes the general prohibition of solely automated decision-making processes that significantly affect individuals and produce legal effects or similarly significantly affect them. This means that when automated decisions have a substantial impact on a data subject's rights, such as denying them a job opportunity or access to services, without any human involvement or intervention, it is generally not allowed.

2. Exceptions to the Prohibition (Article 22(2)):

Despite the general prohibition, Article 22(2) GDPR outlines three exceptions when automated decision-making is permitted even if it significantly affects data subjects:

a. **Necessary for Contractual Performance:** Automated decision-making is allowed if it is necessary for the performance of a contract between the data subject and the data controller. For example, automated credit checks for a loan application may be permitted under this exception.

b. **Authorized by Law with Safeguards:** Automated decision-making is permissible if it is authorized by Union or Member State law, provided that the law includes suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests.

c. **Explicit Consent:** Automated decision-making can be conducted if the data subject has given explicit consent to the process.

3. Safeguard Measures (Article 22(3)):

In cases where automated decision-making is allowed under the exceptions above, Article 22(3) GDPR requires that data subjects have the right to obtain human intervention, express their point of view, and challenge the decision. This means that individuals have the right to request that a human review the automated decision, present additional information, and contest the outcome.

4. Use of Sensitive Data (Article 22(4)):

Article 22(4) GDPR adds an additional layer of protection for sensitive data (also known as special categories of data). It prohibits the processing of sensitive data for automated decision-making unless one of the exceptions mentioned in Article 22(2) applies, or the data subject has explicitly consented to such processing.

In summary, Article 22 of the GDPR aims to protect individuals' rights and freedoms when it comes to automated decision-making processes. While automated decision-making is not outright banned, the GDPR puts strict conditions and safeguards in place to ensure that individuals are not subject to unfair or discriminatory decisions without human oversight and intervention. The use of sensitive data in such processes is also subject to heightened protection and requirements.

3.2.2 California Consumer Privacy Act (CCPA) or California Privacy Rights Act (CPRA) of the United States of America

In the United States of America, this country is the federal state under the Constitution. However, in the Constitution authorized each state to generate the congress and make the own law. In this thesis the author will focus on the California state law which is the leading state enacted the personal data protection law in the US.

In 2020 California Consumer Privacy Act (CCPA)¹⁰⁹ was affected and then in November 2020 the California Privacy Rights Act (CPRA)¹¹⁰ is enacted to extend the provision of CCPA. Most of the CPRA took effect in January 2023.

¹⁰⁹ California Consumer Privacy Act (CCPA)

¹¹⁰ California Privacy Rights Act (CPRA)

3.2.2.1 Definition of Data Processing by Automated Means

Section 1798.140(y) of the California Consumer Privacy Act (CCPA) provides the specific definition of "processing," which encompasses any operation or set of operations conducted on personal information or data, whether such actions are carried out by automated means or not¹¹¹.

3.2.2.2 Data Protection Principles

a. Data Minimization

Under Section 1798.100 (c) of CCPA¹¹², which amended by CPRA, recognized principle of data minimization is an essential aspect of privacy and data protection laws. It helps protect consumer privacy by reducing the risk of excessive data collection and unauthorized use of personal information. Businesses are encouraged to implement data minimization practices to ensure compliance with privacy regulations and respect consumers' privacy rights. By adhering to this principle, businesses can demonstrate responsible data handling practices and build trust with their customers¹¹³.

b. Storage Limitation

The storage limitation provision of the California Consumer Privacy Act (CCPA) under Section 1798.100 (a)(1) and (a)(2)¹¹⁴ of CCPA requires businesses to limit the length of time they retain personal information to no longer than is reasonably necessary for the purpose for which it was collected. This means that businesses should not retain personal information for longer than they need it to provide the goods or services that the consumer has requested, or to comply with legal obligations¹¹⁵.

¹¹¹ California Consumer Privacy Act (CCPA)/ California Privacy Rights Act (CPRA) Section 1798.140(y)

¹¹² California Consumer Privacy Act (CCPA)/ California Privacy Rights Act (CPRA) Section 1798.100(c)

¹¹³ Securiti Research Team, 'What is Data Minimization Under the CPRA?' <<https://securiti.ai/blog/cpra-data-minimization/>> accessed 20 June 2023.

¹¹⁴ California Consumer Privacy Act (CCPA)/ California Privacy Rights Act (CPRA) Section 1798.100 (a)(1) and (a)(2)

¹¹⁵ *supra note 113*

c. Purpose Limitation

This principal places restrictions on the collection and use of personal information by businesses and emphasizes transparency and notice to consumers under Section 1798.100 (a)(3)¹¹⁶.

The purpose limitation principle states that businesses must only collect and use personal information for the specific purposes that they disclosed to consumers when they collected the information. Businesses cannot collect or use personal information for additional purposes that are incompatible with the disclosed purpose without providing consumers with proper notice¹¹⁷.

3.2.2.3 Data Subject Rights

a. Right to Know or Right to Access

The customer has a right to access by requesting to disclose personal data which has collected by data collector and storage from which the personal data is collected. Similarly, the customer could request to know the purpose of the collecting, selling, or sharing personal data.

Some time, the collector transfers their data to third parties, this matter may affect the privacy of the customer. Therefore, thy should have right to know that third person who receive their personal data

Moreover, Section 1798.185(a)(16)¹¹⁸, amended by CPRA, also grants consumers the right to request specific information regarding automated decision-making processes that may affect them.

b. Right to Rectify

By this provision, the customer who are the owner of personal data has the right to request the data collector to correct the inaccurate personal data that the collector shall disclose this right to consumer.

¹¹⁶ California Consumer Privacy Act (CCPA)/ California Privacy Rights Act (CPRA) Section 1798.100 (a)(3)

¹¹⁷ *supra note 113*

¹¹⁸ California Consumer Privacy Act (CCPA)/ California Privacy Rights Act (CPRA) Section 1798.185(a)(16)

To exercise their right to rectify, individuals can contact the business that has collected their personal data and request that the business correct any inaccuracies or incompleteness. The business must correct the information in a commercially reasonable time, but no later than 45 days after the business receives the request.

The right to rectify is an important right that allows individuals to ensure that the personal data that businesses have collected about them is accurate and complete. This is important because accurate and complete personal data is necessary for businesses to provide accurate and personalized services to individuals.

The right to rectify is one of the fundamental rights under the California Consumer Privacy Act (CCPA). It allows individuals to request that a business correct any inaccurate or incomplete personal data that the business has collected about them.

c. Right to Opt-out from Automated Decision-Making and Profiling

This right was accepted by CCPA/CPRA. This principle is right to opt out from the processing the personal data by automated technology and profiling. With this provision the collector shall accept the requests for access to information relevant to the decision-making process and meaning of the possible outcomes of that process regarding to consumers.

The right to opt-out from automated decision-making and profiling is one of the fundamental rights under the General Data Protection Regulation (GDPR). It allows individuals to object to their personal data being used for automated decision-making or profiling purposes.

Automated decision-making is the process of making decisions about individuals without human intervention. This can be done using algorithms or other automated means.

Profiling is the process of using personal data to evaluate certain personal aspects of an individual, such as their interests or behavior.

The right to opt-out from automated decision-making and profiling is set out in Article 22 of the GDPR

d. Right to Deletion

The right to deletion is one of the fundamental rights under the General Data Protection Regulation (GDPR). It allows individuals to request that a data controller delete any personal data that the data controller has collected about them.

To exercise their right to deletion, individuals can contact the data controller that has collected their personal data and request that the data controller delete the data. The data controller must delete the data in a reasonable time, but no later than 60 days after the data controller receives the request.

There are a few exceptions to the right to deletion. For example, the data controller may not be able to delete the data if it is necessary for the data controller to comply with a legal obligation or if the data is necessary for the data controller to establish, exercise, or defend legal claims.

The right to deletion is an important right that allows individuals to control how their personal data is used. By exercising this right, individuals can ensure that their personal data is not kept indefinitely and that they can have a say in how their personal data is used.

e. Right to Opt-out of the Sale or Sharing of Personal Information.

Under the CCPA/CPRA, consumers have the right to opt out of the sale or sharing of their personal information with third parties for the purpose of targeted advertising. This means that consumers can choose to prevent businesses from selling or sharing their personal information with other companies so that they can target them with ads.

To exercise such right to opt out, you can contact the business directly and request to be opted out of the sale or sharing of your personal information. You can also do this online if the business offers an online opt-out option.

f. Right to Data Portability

The right to data portability is one of the privacy rights included in the CCPA/CPRA. Like the GDPR's provision, the CCPA/CPRA's right to data portability allows consumers to obtain and reuse their personal information for their own purposes across different services.

These provisions aim to enhance consumer control over their personal information and provide them with the ability to access and move their data between services seamlessly. The CCPA/CPRA aims to strengthen privacy rights for Californian consumers and increase transparency and accountability for businesses handling personal information.

g. Right to Limit Use and Disclosure of Sensitive Personal Information

The Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information is a provision of the California Privacy Rights Act (CPRA) that gives consumers the right to limit how businesses use their sensitive personal information.

Under the CCPA/CPRA, consumers have the right to direct businesses that collect sensitive personal information about them to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.

This means that businesses are not allowed to use or disclose sensitive personal information for purposes other than those that are necessary to provide the goods or services that the consumer has requested. For example, a business cannot use a consumer's sensitive personal information to market products or services to the consumer unless the consumer has given their consent.

CHAPTER 4

ANALYSIS OF MEASURES OF PERSONAL DATA PROTECTION ON THAI LAW

In the context of machine learning breaches involving personal data security during algorithm training in Thailand, it is essential to understand which laws govern the protection of personal information owners. This chapter will analyze the current laws in Thailand and assess their adequacy in enforcing machine learning training for the protection of personal data. The analysis will be divided into six different categories to provide a comprehensive evaluation of the existing legal framework.

4.1 Problem Concerning Remedial Measure

4.1.1 The Constitution of Thailand

As mentioned in Chapter 3, the right to personal data guaranteed in the Constitution of the Kingdom of Thailand, specifically in Section 32. After considering, it was found that when you want to take advantage of personal information, the constitution stipulated the exception in paragraph 2 that "except by virtue of a provision of law enacted only to the extent of necessity of public interest". This paragraph is a loophole that is difficult to interpret as to which events are considered to be subject to this exception.

The study found that the consideration of such exemptions must be considered that 1) There are the authorized law, 2) It is in the public interest, 3) the action is necessary to achieve the said objective, and 4) the action is proportional to the objective or causes minimal impact considering the action taken.

The study identified that the consideration of such exceptions should be based on whether the law authorizes them and whether they genuinely serve the public interest. Additionally, the actions taken should be necessary to achieve the stated objective and proportionate, causing minimal impact on the individuals concerned.

To address these considerations and carry out the mission of the exceptions to Section 32¹¹⁹, the Personal Data Protection Act (PDPA) was issued. The PDPA is a unique law that allows access to personal data, collection, and use as necessary for the public interest. The PDPA sets limitations and exceptions to protect the rights of individuals as owners of personal data.

However, the study also points out that despite the PDPA's efforts to strike a balance between public interest and individual privacy, there may still be room for interpretation and potential challenges regarding the exceptions imposed on accessing, using, and processing personal data.

4.1.2 Civil and Commercial Code of Thailand

There is doubt that could Section 437 of Thai CCC be applied to the case of personal data infringement?

As provided in Chapter 3, Section 437 sets out the liability of a person who possesses or supervises a vehicle walking with mechanical power for damage caused by the vehicle and persons who have in their possession property that is dangerous by its condition, intent to use, or mechanism. Hence, when consider from the nature of AI and ML which work for the data processing or decision-making, this kind of AI and ML are not the vehicle or property that is dangerous by its condition, intent to use, or mechanism because some of it is software or system form not in form of shaped object. Section 437 might be applied in case of automated vehicle attach causing the damages whether driving with self-driving system or driving by human, as well as in the case of that automated vehicle is under commanded control distantly.

¹¹⁹ Banjerd Singkaneti, Nontawat Nawatrakulpisut, Rewadee Kwanthongyim, Panha Kod Ma Lea Matrakarn Tang Kod Mai Nai Karn Rab Rong Lea Khun Khong Sithi Nai Kwam Pen Yu Suan Tua [Legal Issue and Measure in Relating To Recognize And To Protect The Right To Privacy] (Submitted to Office of the National Human Rights Commission of Thailand) (บรรเจ็ด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์, เรวดี ขวัญทองยี่ม, ปัญหาและมาตรการทางกฎหมายในการรับรอง และคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy)) (เสนอต่อสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ) , p.9-10.

Section 420 might be adequate for personal data infringement more than Section 437. Section 420 could apply in extensive cases because this focus on whatever action to commit wrongful acts and cause damages for individual including any rights of person.

4.1.3 Personal Data Protection Act B.E.2562

According to the *Burke v. Clearview AI, Inc.*, case from the state of California, Clearview AI Inc. was alleged to breach the right to know or right to access under Section 1798.100 of CCPA by utilizing faceprint, as biometric data, of the plaintiff and others in California to train ML named Clearview's facial recognition technology then sells access to the faceprint database to law enforcement agencies and private companies. The complaint charges that Clearview improperly collected personal information without properly notifying consumers. In this case the plaintiff, Mr. Burke, brought the class action case to the southern district of California court because there are more than 100 members of injured persons, and the aggregated value of damages exceeds \$5,000,000 under the 28 U.S. § Code 1332¹²⁰ which is the federal statute of diversity jurisdiction amended by Class Action Fairness Act of 2005¹²¹.

If the case arising in Thailand and the current governed law could be applied for the case.

PDPA, the specific bill for personal data protection, contained the same right to know under CCPA in Section 23 (1). Turning to Civil Procedure Code of Thailand also have the legislation of class action is stipulated in Section 222/1 to 222/49¹²².

As aforesaid, it means that when the case like *Burke v. Clearview AI, Inc.*, case occur in Thailand PDPA Section 23(1) should be adequately applied for that case and the member of injured person could file class action to the court as similar as the US.

¹²⁰ The 28 U.S. § Code 1332

¹²¹ Class Action Fairness Act of 2005

¹²² Civil Procedure Code of Thailand Section 222/1 to 222/49

4.2 Problems Concerning the Definition of Data Processing by Automated Means

Machine learning need the training by input the data then the data will be processed by machine learning. Therefore, machine learning act as the processor. In PDPA is not stipulate the data processing definition in the act clearly. Is consider that it is difficult to construe the meaning on data processing. In PDPA, the mean of data processing is “collection, use, or disclosure” which is very narrow meaning for this circumstance.

In GDPR Article 4 (2) defined the processing is “‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;”. Obviously, GDPR set out widely definition of processing include the processing done by automated technology which is this definition is able to apply to more circumstances than the definition of PDPA absolutely. Especially, the error arising from AI or machine learning is subjected by GDPR explicitly.

In California, USA, known as a technology hub, the specific definition of "processing" can be found in Section 1798.140(y) of the California Consumer Privacy Act (CCPA). This definition includes any operation or set of operations performed on personal information or data, regardless of whether these actions are conducted by automated means or not.

Turn to the narrow meaning of personal data processing under PDPA might be inappropriate in the case to deal with AI or machine learning processing infringe the data privacy of data subject. In this era, the automate technology is very rapid improvement. PDPA should de fine the extensive definition of personal data processing.

4.3 Problems Concerning Data Protection Principles

a. Fairness and Transparency

This is the fundamental principle to protect data privacy from automated technology. When we consider in PDPA will realize that data processing does not mention in PDPA.

However, in GDPR this principle is espoused in Article 5 (1) (a). This principle requires that personal data be processed in a manner that is lawful, fair, and transparent to the data subject. To expand the meaning of transparency is in state in Recital 58, information fairness is specified in Recital 60 and substantive fairness is in Recital 71.

The implicit principles of fairness and transparency may not provide clear guidance on how data processing should be carried out, leading to potential uncertainties and varying interpretations. Data subjects may still face risks related to how their information is handled, and organizations may find it challenging to ensure compliance with data protection requirements.

b. Purpose Limitation

Personal data is the core element in vast set of training algorithm, but the data might be processed in the further purpose beside the purpose that the data owner already consent. The purpose should be scoped to protect the right of data owner.

Thai PDPA only accepts this principle in Section 21 to compresence the purpose of the data owner prior notified to the collector or on the time of the collection. If the new purpose has delivered to the data owner, and the consent is accepted before the time of collection, use, or disclosure, hence it could be done subject to this Act or in other laws.

However, this Section 21 does not specify the exception regarding processing difference from the purpose to be accepted.

c. Data Minimisation

The principle of data minimization emphasizes that organizations should only collect the personal data that is necessary for their intended purposes. They

should limit the amount and extent of data collected to ensure it remains relevant and adequate for the specific purposes.

While the GDPR addresses this principle in Article 5(1)(c) and provides further details in Recital 78, the PDPA, despite being modeled after the GDPR, lacks a specific data minimization principle. Section 22 in the PDPA comes closest to incorporating this principle, but it does not explicitly outline the duties related to data minimization during processing, leaving room for improvement in this aspect.

d. Accuracy

This principle is straight meaning which is the personal data shall be processed accurately. If the processing is inaccurate whatever state of processing that might be affect the propose of the processing and the consent given prior of the data owner, such error should be rectified as soon as possible.

The principle secures the personal data using in machine learning's training because if the personal data from input state is wrong, the outcome might harm the data subject.

This accuracy principle is specified in Article 5(1)(d). However, in PDPA the Section similar to Article 5(1)(d) is Section 35 of the PDPA (Personal Data Protection Act) states that the Data Controller, who is responsible for the collection of personal data, has the duty to ensure that the personal data they hold remains accurate, up-to-date, complete, and not misleading. This means that the Data Controller must take reasonable steps to ensure the accuracy and integrity of the personal data they process.

However, when the author verifies on data processing of personal data, Section 35 obviously not construe to apply this Section to the infringement of data privacy in data processing.

e. Storage Limitation

In GDPR Article 5(1)(e) contain this limitation of storage personal data to protect the personal data which no longer to be processed, should be erased. In PDPA this principle is stipulated in Section 37 (3) the data controller has the duty to put in place an examination system for the erasure or destruction of personal data in certain circumstances.

Specifically, the Data Controller is required to establish a system to review and assess the need for erasure or destruction of personal data when the retention period ends or when the data becomes irrelevant or no longer serves the purpose for which it was collected.

However, the provision in Section 37 is not consider applying for data processing exactly.

4.4 Problems Concerning Data Subject Rights

Upon the consideration by analyzing the governing law of three alternative nations, the author realized that the general data subject rights are recognized by the Thai legislations, especially in PDPA.

However, the author has discovered the significant data subject right regarding automation processing which the right to access to the information regarding the processing of their personal information and what is the outcome of processing by automate technology. Presently, the personal information is the raw material for the AI training and that input and output might be affect the personal data or data owner. Therefore, the data controller shell accepts the request from the data subject. In Thailand, even if PDPA have been stipulated the right to access of data subject in Chapter 3 rights of the data subject.

In Section 30 and Section 31 of the Personal Data Protection Act (PDPA) in Thailand, which outline the rights of data subjects to access their personal data and receive it in a readable format. These provisions establish the following points:

Data subjects have the right to request access to their personal data held by the data controller and the right to request information regarding the source of the data if it was obtained without their consent.

The Data Controller is obligated to fulfill the request, except were permitted by law or pursuant to a court order, and if granting access would adversely affect the rights and freedoms of others.

If the Data Controller rejects the access request, they must record the rejection along with supporting reasons.

If the access request is valid and cannot be rejected based on the reasons provided, the Data Controller must fulfill the request promptly, within a maximum period of thirty days from receiving the request.

The Committee has the authority to establish rules for access requests, including extending the time or implementing other appropriate rules.

On the one hand, Section 31 specifies that data subjects are entitled to receive their personal data from the Data Controller in a readable format commonly used by automatic tools or equipment. They may also request the Data Controller to send or transfer the personal data to other Data Controllers in such formats, if possible.

Regarding the types of personal data that can be accessed, it includes data that the data subject has provided consent for, as well as data exempted from consent requirements under Section 24(3), or any other personal data referred to under Section 24 as prescribed by the Committee.

However, it's important to note that the exercise of these rights may not apply to the sending or transferring of personal data by the Data Controller if it is performed for tasks carried out in the public interest or for compliance with the law, as long as exercising these rights does not violate the rights and freedoms of others. In such cases, the Data Controller must record the rejection of the request with reasons.

Obviously, such act only considers in general situation of personal data processing, the act does not consider about automated processing certainly. As the same issue, if personal data will be processed to train machine learning in Thailand, then data owner need to know the details of their personal data by machine learning, it shall be construed before exercise that right. Because PDPA do not said about this situation explicitly.

Turning to GDPR, the right to obtain information about automated decision-making, including profiling, is embedded in Article 15(1)(h) of GDPR. This Article grants data subjects the right to confirm whether their personal data is being processed and, if so, to access that data and obtain specific information, including the existence of automated decision-making.

4.5 Problems Concerning Rights Specific on Automated Means

Upon the research on the right specific to automate means analyzing with GDPR and CCPA/CPRA and Thai law, it has been found the lack of rights focusing on automation processing. The author classifying such rights to 2 categories which are rights to information and rights to explanation as follows:

4.5.1 Right to Information Specific on Automated Means

The right to information or the data subject's right to be informed has the same principle to right to access about the existence of AI or machine learning processes and their potential effects and consequences is essential for ensuring transparency and accountability in data processing. However, this principle can pose challenges due to the difficulty in understanding the information generated during AI processing, often referred to as the "Black box" problem.

Despite the significance of AI and its impact on data processing, the PDPA in Thailand does not currently have explicit provisions addressing the right to information or the data subject's right to be informed of existing of AI or data processing. This absence could lead to uncertainties and complexities in regulating AI-related data activities under the PDPA.

4.5.2 Right to Explanation Specific on Automated Means

The right to explanation known as specific right of data protection by automated means processing under GDPR and this is accepted by several countries. However, in PDPA of Thailand does not recognize the principle of right to explanation.

As mentioned in Chapter 3, the right to explanation is contained in GDPR Article 22(3) as suitable safeguard measures which are (1) right to obtain human intervention, (2) right to express point of view, and (3) right to challenge the decision, and in Recital 71 are (1) Specific Information, (2) Right to obtain human intervention, (3) right to express point of view, (4) right to obtain an Explanation, and (5) right to challenge the decision.

For such rights is rely on the error protection of automated decision-making or AI processing which is the input and output are able to cause the mistake. Thus, if

the data controller wishes to process the personal data by AI or machine learning, the data controller needs to grant the data subject to design the process with their intention because the material that the data controller use in training machine learning or make-decision by automate technology is the personal data of each data subject. On the other hand, the right to obtain human intervention is the way to prevent the mistake or error of algorithm from the reason that the suggestion of some algorithmic science is the AI shall co-operate with human to supervise the process of AI.

Notwithstanding, PDPA also without the right to explanation regarding the AI or machine learning as the standard measures to protect the data subject from automated decision-making and automation processing. We should protect the data security by recognize the right of the data owner to exercise the right to intervention in the personal data processing.

4.6 Problems Concerning Automate Decision-Making or Automated Processing Provision

Article 22 of the GDPR concerns on general prohibition of solely automated decision-making processes that significantly affect individuals and produce legal effects or similarly significantly affect them, including profiling, if that decision produces legal effects concerning them or similarly significantly affects them. This means that if a decision is made solely through automated processing without any human involvement, and it has a legal or significant impact on the data subject, they have the right to avoid being subjected to such a decision.

In CCPA/CPRA also generate the same principle on the right base calls right to opt-out from automated decision-making and profiling under Section 1798.185 (16).

Some people might doubt that why the data subject does not want to be process his or her personal data by automated technology because when the data subject already give consent to data controller for processing, the data controller is independent to select the processing by general or automated technology. However, if we consider that the general and automated technology is totally difference, the

law could not deem both ways are the same thing. Hence, GDPR open for the decision of data subject fairly.

As mentioned above, Article 22 (3) of the GDPR recognizes the right to explanation. The author agrees that PDPA should provide the specific provision in relating to automate decision-making and automation processing for the data subject in Thailand.

On the other hand, Thai PDPA do not wrote regarding automate processing technology in this act certainly. The author has found that PDPA might face with the trouble of legal interpretation when the automated technology participates in the infringement data privacy case held in Thailand. GDPR consider that the data subject should exercise the right to design their consent throughout the process, the law should not grant the data controller override the data owner by the adhesion form of process.

Overall, it is evident that the existing legal framework in Thailand concerning the protection of personal data during machine learning training is not as comprehensive and explicit as in some other jurisdictions like GDPR and CCPA/CPRA. Addressing these issues and incorporating more specific provisions for automated processing and data subject rights will be essential to ensure effective protection of personal data during machine learning activities in Thailand.

The author also identifies the differences observed during the comparative analysis of each country in Table 1.

Tables 4.1 A Comparative Study of Personal Data Protection Measures

Rights Countries	European Union GDPR	The United States of America CCPA/CPRA	Thailand PDPA
Definition	Article 4 (2)	Section 1798.140 (y)	None
Data Protection Principles	<ol style="list-style-type: none"> 1. Fairness and Transparency 2. Purpose Limitation 3. Data Minimisation 4. Accuracy 5. Storage Limitation 	<ol style="list-style-type: none"> 1. Data Minimization 2. Storage Limitation 3. Purpose Limitation 	<ol style="list-style-type: none"> 1. Fairness and Transparency 2. Purpose Limitation 3. Data Minimisation 4. Accuracy 5. Storage Limitation <p><i>Remark: the data protection principle in PDPA is not regarding processing.</i></p>
Data Subject Rights	<ol style="list-style-type: none"> 1. Right to Access Right to Data Portability 2. Right to Object to Processing of Personal Data 3. Right to Objecting to Profiling for Marketing 4. Right to Objecting to Processing for Research 5. Right to Erasure 	<ol style="list-style-type: none"> 1. Right to Know or Right to Access 2. Right to data portability 3. Right to Deletion 4. Right to Rectify 5. Right to Opt-out of the Sale or Sharing of Personal Information. 6. Right to Limit Use and Disclosure of Sensitive Personal Information 	<ol style="list-style-type: none"> 1. Right to Be Informed 2. Right to Access 3. Right to Data Portability 4. Right to Object 5. Right to Erasure 6. Right to Restrict Processing 7. Right to Rectification 8. Right to Withdraw Consent

Rights Specific on Automated Means	<ol style="list-style-type: none"> 1. Right to Information 2. Right to Explanation <ol style="list-style-type: none"> 1. Specific Information 2. Right to Obtain Human Intervention 3. Right to Express Point of View 4. Right to Obtain an Explanation 5. Right to Challenge the Decision 	Right to Opt-out From Automated Decision-Making and Profiling	<p>None</p> <p>Remark: The right to be informed is similar to the right to information, but it does not concern automated means.</p>
Automate Decision-Making or Automated Processing Provision	<p>Article 22 Automated individual decision-making, including profiling</p> <p><i>Remark: "right not to be subject to a decision based solely on automated processing" in paragraph 1, even uses the word "right" but this is more about prohibition for the data controller.</i></p>	<p>None</p> <p><i>Remark: The right to opt-out from automated decision-making and profiling under CCPA/CPRA is not deemed to be on the legal prohibition, but it is deemed to be on the data subject right base.</i></p>	<p>None</p>

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

The era of AI development requires continuous practice and refinement of algorithms. One such algorithm, known as machine learning, is considered the intelligent brain of AI. Machine learning enables computers to learn from data and improve their performance over time. In this process, data science or computer science experts input datasets to machine learning systems, allowing them to process the data and derive appropriate outcomes.

In this thesis, the author examines six different problems related to the appropriate measures for personal data protection in the context of automatic processing. These issues include remedial measures for data subjects, the definition of automated processing, the recognition of data protection principles, the acknowledgment of data subject rights, the identification of specific rights for automated means, and the need for specific provisions concerning automated processing. This chapter aims to summarize the findings of the comparative research conducted on these topics.

5.1.1 Remedial Measure

The research shows that the right to privacy is accepted in the Constitution of Thailand and Personal Data Protection Act B.E. 2562 was issued to extend and to recognize the personal data protection measures for Thai citizen. The person who are injured of personal data protection infringement under PDPA, they have a right to bring the lawsuit to the court claiming for any damages. The Civil and Commercial Code of Thailand Section 420 could be applied to the infringement of data subject right also. In addition, the class action procedure also could be applied to the case which have vast amount of injured person like data infringement case from training marching learning or automatic processing.

Even though data subject could remedy any damages as the first paragraph said, but the rights of data subject, data protection principle, and specific provision in relating to automatic processing shall be recognized in Thai applicable law.

5.1.2 Definition of Data Processing by Automated Means

Despite to fact that under the Thai legislation does not have the precise definition of data processing by automated means and the current implicit definition of data processing is incomprehensive, the occurrence of personal data infringement by the processing of machine learning would have no precise identification under the law. Hence, The Thai's PDPA should defined fine the extensive definition of data processing by automated means on order to simplify the legal interpretation.

5.1.3 Data Protection Principles

In conclusion, while the Personal Data Protection Act (PDPA) of Thailand acknowledges fundamental data protection principles, it falls short in explicitly addressing data processing, particularly concerning automated means. Although the PDPA lays the groundwork for data protection measures, it lacks specific provisions that comprehensively govern data processing activities.

This loophole could potentially lead to uncertainties in how organizations handle personal data using automated technologies and may leave data subjects vulnerable to privacy risks.

The absence of explicit regulations regarding data processing presents a gap in the current Thai legislation framework. This loophole could potentially lead to uncertainties in how organizations handle personal data using automated technologies and may leave data subjects vulnerable to privacy risks.

5.1.4. Data Subject Rights

PDPA of Thailand provided the general data subject rights in the act. Especially, the effective right, which is the right to access, are recognized under PDPA. This means that the data subject can exercise the right to access to the information of data processing. However, the right to access should be extended to the apply with information of the automated means' intervention.

5.1.5. Rights Specific on Automated Means

Firstly, PDPD recognizes the general right to be inform which is the same principle of right to information. However, right to information specific on automated processing is absented under PDPA. Thus, right to be inform under Section 23 of PDPA should be stipulated the automatic processing in the provision in order to the certification of data protection measure in relating to automatic processing.

Secondly, the right to explanation for personal data protection does not exist in any Thai legislations, this loophole should be fulfilled by recognition of such specific right to guarantee the security of personal data protection in relating to machine learning processing.

5.1.6. Automate Decision-Making or Automated Processing Provision

The legislation to prohibit the sole automatic processing on personal data that affects the data subject or, on the other hand, the right to opt-out of automatic processing is an important measure for personal data protection regarding automatic processing which does not exist in PDPA. However, the current legislation is insufficient to personal data infringement in relating to automatic processing. Hence, the principle should be recognized in Thai's legislation.

5.2 Recommendations

As the author have mentioned above, the Personal Data Protection Act of Thailand may not be adequate to address the specific challenges related to the protection of personal data in the context of machine learning. To address this gap and improve the basic principles of personal data protection, the author may recommend the following solutions:

5.2.1 Definition of Data Processing by Automated Means

In order to enhance the comprehensive of processing by automated means under PDPA and expand the enforcement of current provisions under PDPA, the author would suggest that Thailand should amend 2 definitions under PDPA including the terminology of Data Controller and Data Processor and escalate the

terminology of Processing in Section 6 with the details that “processing” means an operation which is performed on personal data, whether or not by automated means, such as collection, use, or disclosure of the Personal Data as;

a. ““Data Controller” means a Person or a juristic person having the power and duties to make decisions regarding the processing, collection, use, or disclosure of the Personal Data;”

b. ““Data Processor” means a Person or a juristic person who operates in relation to the processing, 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;”

“ “Processing” means operation or set of operations which is performed on personal data or on sets of personal data including collection, use, or disclosure of the Personal Data, whether or not by automated means.”

5.2.2 Data Protection Principles

In order to recognize the fundamental data protection principle regarding data processing in the specific legislation in Thailand as the general protection measure of data subject, The author would suggest that Thailand should amend the provision regarding the processing in PDPA by increasing Section 21/1 under Chapter 2 regarding personal data protection of PDPA separately.

The author would suggest as follows:

“Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes under Section 24 and 26 shall not be considered to be incompatible with the initial purposes.

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes under Section 24 and 26”

5.2.3 Data Subject Rights

The right to access to the information of data processing is the very important right for data subject because the one who are processed his/her own personal data for any purposes, he/she should have right to access to that information regarding the processing, especially when the personal data would be processed by automatic technology. Hence, the right to access should be amended

The author would suggest that Thailand should add the right to access for data subjects’ enhancement in PDPA by amendment Section 30, paragraph 1 and adding Section 31/1 under Chapter 2 regarding the rights in data subject of PDPA.

The author would suggest as follows:

“The data subject is entitled to request access to and obtain copy of the Personal Data related to him or her, which is under the responsibility of the Data Controller, or to request the disclosure of the acquisition of the Personal Data obtained without his or her consent, including the existence of automated processing as well as the significance and the envisaged consequences of such processing for the data subject.”

This right to access is the active way of exercising of the right from data owner because the data subject deserves the right to know everything regarding the processing of their personal information. PDPA should be add Section 31/1 under Chapter 2 regarding the rights in data subject of PDPA as.

“The data subject shall have the right to know whether personal data is being processed. and access to information about data processing by automated means. as well as the significance and the consequences of such processing for the data subject.”

5.2.4 Rights Specific on Automated Means

These specific rights should accept in Thai legislation to protect the data subject as the appropriate measure for personal data protection from machine learning as follows:

a. Right to Information Specific on Automated Means

This specific right has similar purpose with the right to be inform because it specifies on the duties of data collector regarding to inform the data owner of the existence of machine learning processing and its affect data subject.

Upon PDPA already have the right to be inform stipulated in Section 23, the author, therefore, would like to suggest the amendment of Section 23 by increase (7) as the duty to inform the data subject in relating to existence of automatic processing as.

“(7) Data Processing by automated means as well as the significance and the consequences of such processing for the data subject.”

b. Right to Explanation Specific on Automated Means

Pursuant to conducting comparative legal research, the author has found the supreme benefit of the right to explanation which could provide the appropriate level of personal data protection in Thailand. Therefore, the author would suggest that Thailand should accept the right to explanation to the personal data protection legislation.

Upon PDPA of Thailand do not accept the right to explanation yet, the author would agree to espouse the separated Section 31/2 under Chapter 2 regarding the rights in data subject of PDPA as.

“Upon the personal data shall be processed by automated means, the data subject shall be subject to safeguard rights at least as follow.

1. right to be provided specific information;
2. right to obtain human intervention;
3. right to express his or her point of view;
4. right to obtain an explanation of the decision reached after such assessment;
5. right to challenge the decision.”

5.2.5 Automate Decision-Making or Automated Processing Provision

As aforesaid, the specific provision for automated decision-making or automated processing compresence the risk from the automatic processing by provide the measure for data subject from automatic processing whether in data subject right form or duty form.

This method is quite significance for appropriate measure of personal data protection. Therefore, the author would like to suggest amending the PDPA by accepting such measure to Thai legislation. According to comparative legal conduct, the author agrees to go with create the duty to the data controller and data processor to provide the safeguard measure to the data subject by add Section 42/1 under Chapter 2 regarding the rights in data subject of PDPA as.

“The data subject shall not to be subject based solely on automated processing as well as be provided the meaningful information which in relating to legal effects concerning him or her or similarly significantly affects him or her.”

In conclusion, this thesis focuses on a comparative research study aimed at identifying appropriate measures for personal data protection in the context of artificial intelligence processing under Thai law, with a specific focus on machine learning. The research conducted solely pertains to measures related to personal data protection and does not delve into liabilities or compensations.

While the measures discussed in the thesis may not be fully adequate for ensuring comprehensive personal data protection, they serve as a foundational framework for such protection. However, it is crucial to gather and implement these measures using ethical methods in artificial intelligence to ensure a high standard of personal data protection. Ethical considerations play a significant role in safeguarding individuals' privacy and ensuring responsible data handling practices within the realm of AI and machine learning.

REFERENCES

Books

A. M. Turing, 'COMPUTING MACHINERY AND INTELLIGENCE'

European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence

European Union Agency for Fundamental Rights, Handbook on European data protection law 2018 Edition

Independent High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Disciplines' (2019)

Jit Setabutr, Lak Kod Mai Pheang Laksana La Merd [Principles of Law on Torts] (8th edition, Faculty of Law, Thammasat University, 2013) (จิต เศรษฐบุตตร, หลักกฎหมายแพ่ง ลักษณะละเมิด (พิมพ์ครั้งที่ 8, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2556))

Sanankorn Sotthibandu, Kham Athibai Kod Mai Laksana La Merd Chat Kan Ngan Nok Sang Lea Lab Mi Kuan Dai [Explanations of Civil and Commercial Code oh Torts, Agency Without Specific Authorizations Undue Enrichment] (rd edition, Winyuchon, 2010) (ศันนัทกรณ โสทธิพันธ์, คำอธิบายกฎหมายลักษณะละเมิดจัดการงานนอกสิ่งละลวมมิควรได้ (พิมพ์ครั้งที่ 3, วิญญูชน 2553))

Thomas D. Grant and Damon J. Wischik, 'On the path to AI: Law's prophecies and the conceptual foundations of the machine learning age' (2020), P.X Prologue.

Tom M Mitchell, 'Machine Learning' March 1, 1997

William J. Raynor, Jr., 'The International Dictionary of Artificial Intelligence (1999)

Articles

Avijeet Biswal, '7 Types of Artificial Intelligence That You Should Know in 2023'

Bhumindr Butr-Indr, Law and Artificial Intelligence (AI), Thammasat Law Journal, Vol.47 No.3 (September 2018) (ภูมิินทร์ บุตรอินทร์, กฎหมายกับปัญญาประดิษฐ์, วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, ปีที่ 47 ฉบับที่ 3 (กันยายน 2561))

Bhumindr Butr-Indr, Silver Economy, Robotic, Artificial Intelligence and Law. Thai Network Information Center Foundation, (2020) (ภูมิินทร์ บุตรอินทร์, เศรษฐกิจสีเงิน หุ่นยนต์ ปัญญาประดิษฐ์กฎหมาย, มุลนิธิ สารสนเทศเครือข่ายไทย (2563))

Council of Europe, 'History of Artificial Intelligence'

Dr. Nakorn Serirak, Kwam Pen Suan Tua Pai Tai Rattathanmanoon Mai Tong Jap Ta (ดร. นคร เสรีรักษ์, ความเป็นส่วนตัวภายใต้รัฐธรรมนูญใหม่ "ต้องจับตา")
< <https://ilaw.or.th/node/4255>> accessed 20 June 2023.

European Commission, 'Can I be subject to automated individual decision-making, including profiling?'

John McCarthy, 'WHAT IS ARTIFICIAL INTELLIGENCE?'

Katrina Wakefield, 'A guide to the types of machine learning algorithms and their applications'

Theses and Dissertations

Janewit Panichraksapong, 'Legal Liability of Damage from Drones' (Master of Laws Degree Thesis, Thammasat University 2019)

Paranya Angsusingha, ‘Legal Measures for Personal Data Protection Regarding Automated Decision-Making in The Private Sector’ (Master of Laws Degree Thesis, Thammasat University 2021)

Sittaphuthathatthep Jakraphopmahadecha, Karn Khum Krong Kho Moon Suan Book Khon Koranee Sueksa Karn Pra Muan Phon Kho Moon Doi Panya Pradit [Personal Data Protection in Case Study of Artificial Intelligence’s Processing] (Master of Laws Degree Independent Study, University of the Thai Chamber of Commerce 2018) (สิทธิระพุทธทาสเทพ จักรภพมหาเดชา, การคุ้มครองข้อมูลส่วนบุคคลกรณีศึกษาการประมวลผลข้อมูลโดยปัญญาประดิษฐ์ (Artificial Intelligence: AI)) (การค้นคว้าอิสระ ปริญญานิติศาสตร์มหาบัณฑิต มหาวิทยาลัยหอการค้า 2561)

Project Reports

Banjerd Singkaneti, Nontawat Nawatrakulpisut, Rewadee Kwanthongyim, Panha Kod Ma Lea Matrakarn Tang Kod Mai Nai Karn Rab Rong Lea Khun Khong Sithi Nai Kwam Pen Yu Suan Tua [Legal Issue and Measure in Relating To Recognize And To Protect The Right To Privacy] (Submitted to Office of the National Human Rights Commission of Thailand) (บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์, เรวดี ขวัญทองยิ้ม, ปัญหาและมาตรการทางกฎหมายในการรับรอง และคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy)) (เสนอต่อสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ)

Bhumindr Butr-Indr, Kho Moon Suan Book Khon Tam Neaw Pra Ti Bat 1/2020 Nai Karn Pra Muan Phon Kho Moon Suan Book Khon Nai Bo Ree Bot Khong Yarn Pha Ha Na Tee Cheam Tor Lea Karn Klearn Vai Tee Keaw Khong Kab App Pli Ke Chan Khong Ka Na Kam Ma Karn Kho Moon Suan Book Khon Khong Yu Rop [Personal Data by “Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications” of The European Data Protection Board] (Submitted to The Research Promotion Committee, Faculty of Law, Thammasat University 2023) (ภูมินทร์ บุตรอินทร์, ข้อมูลส่วนบุคคลตาม “แนวปฏิบัติ 1/2020 ในการประมวลผลข้อมูลส่วนบุคคลในบริบท

ของยานพาหนะที่เชื่อมต่อ และการเคลื่อนไหวที่เกี่ยวข้องกับแอปพลิเคชัน” ของคณะกรรมการข้อมูลส่วนบุคคลของยุโรป) (เสนอต่อคณะกรรมการส่งเสริมงานวิจัยคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ กรกฎาคม 2566)

Bhumindr Butr-Indr, Pra Den Tha Tai Tang Dan Kod Mai Nai Yook : IOTs Suk Sa Kor Ra Nee Kwam Rab Phid Jak Karn Chai Ngang Smart Car [Legal Challenges in the IOTs: Case Study of Smart Car Liability] (Submitted to The Research Promotion Committee, Faculty of Law, Thammasat University 2020) (ภูมินทร์ บุตรอินทร์, ประเด็นท้าทายทางด้านกฎหมายในยุค: IOTs ศึกษากรณีความรับผิดจากการใช้งาน Smart Car) (เสนอต่อคณะกรรมการส่งเสริมงานวิจัยคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ กรกฎาคม 2563)

John McCharthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon, ‘A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence’

Websites

‘GDPR Personal data’ < <https://gdpr-info.eu/issues/personal-data/> > accessed 26 March 2023.

‘What id personal data?’ <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> accessed 26 March 2023.

A. M. Turing, ‘COMPUTING MACHINERY AND INTELLIGENCE’ <<https://www.csee.umbc.edu/courses/471/papers/turing.pdf>> accessed 6 January 2021.

Abi Tyas Tunggal, ‘What is Sensitive Data?’ < <https://www.upguard.com/blog/sensitive-data> > accessed 20 June 2023.

Alexandros Zenonos, PhD, ‘Artificial Intelligence and Data Protection Two sides of the same coin’ <<https://towardsdatascience.com/artificial-intelligence-and-data-protection-62b333180a27>> accessed 23 December 2022.

ALTURIS, '4 TYPES OF ARTIFICIAL INTELLIGENCE: TYPE I - REACTIVE MACHINES'
<<https://www.alturis.ai/post/4-types-of-artificial-intelligence-type-i-reactive-machines>>
accessed 25 March 2023.

Amit Ray, 'AI Winter: The Highs and Lows of Artificial Intelligence' <
<https://www.historyofdatascience.com/ai-winter-the-highs-and-lows-of-artificial-intelligence/>> accessed 20 June 2023.

Arend Hintze, 'Understanding the four types of AI, from reactive robots to self-aware beings' <<https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616> > accessed 25 March 2023.

Avijeet Biswal, '7 Types of Artificial Intelligence That You Should Know in 2023'
<https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/types-of-artificial-intelligence#types_of_artificial_intelligence > accessed 25 March 2023.

B.J. Copeland, 'artificial intelligence'
<<https://www.britannica.com/technology/artificial-intelligence>> accessed 15 December 2021.

B.J. Copeland, 'DENDRAL expert system'
<<https://www.britannica.com/technology/DENDRAL>> accessed 20 June 2023

Ben Lorica and Mike Loukides, 'How AI and machine learning are improving customer experience' <<https://www.oreilly.com/radar/how-ai-and-machine-learning-are-improving-customer-experience/>> accessed 15 December 2021.

Bernard Marr, 'What are the Four Types of AI?' <<https://bernardmarr.com/what-are-the-four-types-of-ai/>> accessed 25 March 2023

Brandon Vigliarolo, 'Amazon Alexa: Cheat sheet'

<<https://www.techrepublic.com/article/amazon-alexa-the-smart-persons-guide/> >
accessed 20 June 2023.

Cambridge Dictionary,

'Data' <<https://dictionary.cambridge.org/dictionary/english/data>> accessed 15
December 2021.

Center For Strategic & International Studies, Biometrics and Security

<<https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity-6>> accessed 15 December 2021.

Council of Europe, 'History of Artificial

Intelligence' <<https://www.coe.int/en/web/artificial-intelligence/history-of-ai>>
accessed 6 January 2021.

Coursera, '4 Types of AI: Getting to Know Artificial Intelligence'

< <https://www.coursera.org/articles/types-of-ai> > accessed 20 June 2023.

Craig Stedman, 'data mining'

<<https://www.techtarget.com/searchbusinessanalytics/definition/data-mining> >
accessed 20 June 2023.

David Gewirtz, ' Volume, velocity, and variety: Understanding the three V's of big data' <<https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/> > accessed 20 June 2023.

ELIZA: a very basic Rogerian psychotherapist chatbot

<<https://web.njit.edu/~ronkowitz/eliza.html> > accessed 20 June 2023.

Elle Poole Sidell, 'What Does Google Do With Your Data?' <<https://www.avast.com/c-how-google-uses-your-data#gref>> accessed 15 December 2021.

European Commission, 'Can I be subject to automated individual decision-making, including profiling?' <https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_en> accessed 20 June 2023.

European Commission, 'What is personal data?' <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> accessed 26 March 2023.

Evan Pu, 'Understanding OpenAI Five' <<https://evanthebouncy.medium.com/understanding-openai-five-16f8d177a957> > accessed 20 June 2023.

IBM, 'A Computer Called Watson' <<https://www.ibm.com/ibm/history/ibm100/us/en/icons/watson/> > accessed 20 June 2023.

IBM, 'Deep Blue' < <https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/> > accessed 20 June 2023.

IBM, 'What is machine learning?' < <https://www.ibm.com/topics/machine-learning> > accessed 25 March 2023.

Import.io, 'What is data, and why is it important?' <<https://www.import.io/post/what-is-data-and-why-is-it-important/>> accessed 5 September 2021.

intersoft consulting, 'GDPR Personal data' < <https://gdpr-info.eu/issues/personal-data/> > accessed 26 March 2023.

Jack Schofield, 'Computer chatbot 'Eugene Goostman' passes the Turing test' <<https://www.zdnet.com/article/computer-chatbot-eugene-goostman-passes-the-turing-test/>> accessed 20 June 2023.

Jack Vaughan, 'Data'

<<https://searchdatamanagement.techtarget.com/definition/data#:~:text=In%20comp%20data%20is%20information,converted%20into%20binary%20digital%20form.&text=Raw%20data%20is%20a%20term,its%20most%20basic%20digital%20format>> accessed 15 December 2021.

John McCarthy, 'WHAT IS ARTIFICIAL INTELLIGENCE?' <<http://www-formal.stanford.edu/jmc/whatisai/node1.html>> accessed 13 March 2022.

John McCharthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence' <<http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>> accessed 20 June 2023.

Katrina Wakefield, 'A guide to the types of machine learning algorithms and their applications' <https://www.sas.com/en_gb/insights/articles/analytics/machine-learning-algorithms.html> accessed 26 March 2023

Lee Johnston, 'Recent cases Highlight Growing Conflict Between AI and Data Privacy' <<https://www.haynesboone.com/news/publications/recent-cases-highlight-growing-conflict-between-ai-and-data-privacy>> accessed 1 April 2023.

Marc Dimmick, 'How the Variety in Big Data Works as an Advantage' <<https://opengovasia.com/how-the-variety-in-big-data-works-as-an-advantage/>> accessed 20 June 2023.

Mark Labbe and Ivy Wigmore, 'narrow AI (weak AI)'

<<https://www.techtarget.com/searchenterpriseai/definition/narrow-AI-weak-AI>>
accessed 25 March 2023.

Paphamon Arayasukawat, 'COVID-19 Vaccination Drive Will Prioritize Social Security
Section 33

Employees' <https://thainews.prd.go.th/en/news/print_news/TCATG210520115043858
.> accessed 15 December 2021

Priyadharshini, 'What Is Machine Learning and How Does It Work?'

<<https://www.simplilearn.com/tutorials/machine-learning-tutorial/what-is-machine-learning>> accessed 15 December 2021.

Professor Christopher Manning, 'Artificial Intelligence Definition'

<<https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf>> accessed
26 August 2022.

PWC, 'Thailand's Personal Data Protection Act (PDPA): are companies in Thailand
ready?' <<https://www.pwc.com/th/en/tax/personal-data-protection>

act.html#:~:text=Thailand's%20Personal%20Data%20Protection%20Act%20BE%20256
2%20 PDPA)%20will%20come,before%20and%20after%20the%20deadline.>
accessed 15 December 2021

Rickie Walker, 'Timeline of Artificial Intelligence AI — 2022 Update' <

<https://appmaster.io/blog/timeline-artificial-intelligence-ai-2022-update> > accessed 20
June 2023.

Rockwell Anyaho, 'The History of Artificial Intelligence'

<<https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/>> accessed 6
January 2021

Roshni Lokare, 'Type 2 of Functional AI — Limited Memory AI'

<<https://medium.com/appengine-ai/type-2-of-functional-ai-limited-memory-ai-e687ffed6b1e> > accessed 25 March 2023.

Sara Brown, 'Machine learning, explained' < <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained> > accessed 25 March 2023

Securiti Research Team, 'Data Privacy Laws and Regulations Around the World'

<<https://securiti.ai/data-privacy-laws/> > accessed 20 June 2023.

Shaan Ray, 'History of AI' <<https://towardsdatascience.com/history-of-ai-484a86fc16ef>> accessed 6 January 2021.

Sumeet Bansal, 'What Are the Key Characteristics of Big Data?'

<<https://www.analytixlabs.co.in/blog/characteristics-of-big-data/>> accessed 20 June 2023.

Victor Sanchez, 'The history of Siri and its impact on today's technology' <

<https://blog.routinehub.co/the-history-of-siri-and-its-impact-on-todays-technology/> > accessed 20 June 2023.

Vijay Kanade, 'Narrow AI vs. General AI vs. Super AI: Key Comparisons'

<<https://www.spiceworks.com/tech/artificial-intelligence/articles/narrow-general-super-ai-difference/>> accessed 25 March 2023.

Vijay Kanade, 'What Is General Artificial Intelligence (AI)? Definition, Challenges, and

Trends' < <https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-general-ai/>> accessed 25 March 2023.

Vishupriya Chandrasekar, 'Theory of Mind AI'

<<https://www.linkedin.com/pulse/theory-mind-ai-vishnupriya-chandrasekar> >

accessed 25 March 2023.

Vox of Dartmouth, 'Artificial Intelligence (AI) Coined at Dartmouth'

<<https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth>>

accessed 6 January 2021.

Legislations

California Consumer Privacy Act 2018

California Privacy Rights Act 2020

Civil and Commercial Code B.E. 2468 (1925)

Civil Procedure Code B.E. 2477 (1934)

Class Action Fairness Act of 2005

Constitution of the Kingdom of Thailand B.E. 2560 (2017)

Electronic Transactions Act B.E. 2544 (2001)

General Data Protection Regulation 2018

Official Information Act B.E. 2540 (1997)

Personal Data Protection Act, B.E. 2562 (2019)

Cases Law

Burke v. Clearview AI, Inc., Case No.: 3:20-cv-00370-BAS-MSB (S.D. Cal.)

BIOGRAPHY

Name	Kittitach Mana
Date of Birth	December 28, 1990
Educational Attainment	Academic Year 2012: Bachelor of Laws, Thammasat University
Work Position	Partner Khalid Chambers Co., Ltd.

