Spring 2020

The Impact of Artificial Intelligence on Data Protection: A Legal Analysis

Ana Paula Dos Santos
anapauladosantos.adv@gmail.com

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DATA PROTECTION: A LEGAL ANALYSIS

By

Ana Paula dos Santos

A Thesis Submitted to the McGeorge School of Law

In Partial Fulfillment of the

Requirements for the Degree of

MASTERS OF LAWS

McGeorge School of Law
Transnational Business Practice

University of the Pacific
Sacramento, California

2020

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DATA PROTECTION: A LEGAL ANALYSIS

By

Ana Paula dos Santos

APPROVED BY:

Thesis Advisor: Michael S. Mireles, J.D.

DEDICATION

I dedicate this master's thesis to my mom, who taught me how to dream and work hard for everything I dreamt about. These lessons revealed a world full of amazing opportunities and possibilities without any barriers. Thank you, mom, for giving me more than life: the possibility to improve as a human every single day. For my brother Pablo and my sister in Law Rita – my loved ones. For all of my relatives and close friends who kept me in their prayers and sent good energy.

I believe that what makes my journey here unique and fascinating are the people who worked with me, and in so many ways, helped me to achieve my goals. They are part of my life story, and I will always be here for each one of them.

For Theo van der Loo who saw what many people could not see, thank you so much for the encouragement, mentoring, friendship, and everything you have been doing to make it real.

For Maria Regina Araujo who enthusiastically worked with me during all of my master's thesis writing. Thank you so much.

For Stefan Schubert a friend who always has reserved some time to listen to me or advise me. Thank you.

For Bryan Scholes, I will never forget the beginning because you were there not only giving me English classes but also your friendship. And, for Lana Marion, thank you for providing so many ways to join you and Bryan to effectively learn the language. “It is my time.”

For Mrs. Kao and Alyce, my English teachers from Los Angeles who devoted time to teach me the language in mindful ways.

For Bhante Seelaratana, a wonderful and supportive friend who always is sharing wisdom and peace.

ACKNOWLEDGMENTS

I would like to express my sincere thanks to my supervisor Professor Michael S. Mireles who sent me materials and shared thoughtful comments, which helped me improve my thesis a lot, gave me confidence and space to work, and always answered my requests in a short amount of time.

I also would like to express my deep and sincere gratitude to my friend and mentor, Professor Kojo Yelpaala who gave me the seeds to start the process of deep learning and thinking. The idea of this master thesis was born in Professor Kojo Yelpaala's office when he taught his last course on International Business Transactions before his retirement. I was privileged to meet him as his student. He provided me with the opportunity to discover a new world where determination, focus, and wisdom are vital to achieve short and long term goals. I will never be able to return to Professor Yelpaala the rich seeds, full of the knowledge that he shared with me during this period. Thank you so much.

I thank everyone from the McGeorge School of Law, in particular Ms. Clemence Kucera and Ms. Jocelyn Blinn who always reserved time to meet with me in their office, providing feedback on everything they could.

I thank Ms. Molly Rentscher from the writing support center who gave me support and encouragement to write and improve each day.

I would like to thank the library team, especially Mrs. Sandra Burdi who solicited materials from other libraries. I also thank Mr. Dan Breuer for all his help with my computer and Mr. Paul Howard for always providing feedback on research materials and citation formats.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DATA PROTECTION: A LEGAL ANALYSIS

Abstract

By Ana Paula dos Santos

University of the Pacific
2020

This study explores the implications of artificial intelligence innovation on privacy, data protection regulations, and other related laws. With the spread of data endangering privacy, it is a difficult task to protect the "right to be let alone," considered as an individuals' liberty and a fundamental right. This research has shown that at the same time, the use of personal information by artificial intelligence can impact an individual's privacy. Artificial intelligence also brings conjecturable, incredible, and useful innovation that benefits humans. The analysis of the enacted laws in the European Union, China, and the United States on data protection regulations demonstrates that the laws are not sufficient to prevent the challenges raised by artificial intelligence. This thesis discusses the great importance of the subject matter to society, the several impacts it can foment and the lack of regulations to avoid the outcome.

Keywords: Artificial Intelligence – Privacy – Data Protection- – Technology – Personal Data

TABLE OF CONTENTS

LIST OF TABLES

Table

LIST OF FIGURES

Figure

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AG	Attorney General
AGI	Artificial General Intelligence
APP	Application
EU	European Union
CA	Cyberspace Administration of China
CCPA	California Consumer Privacy Act
CSL	Cybersecurity Law
COPPA	Children’s Online Privacy Protection Act
DDPA	Driver’s Privacy Protection Act
DPAs	Data Protection Authorities
FACTA	Accurate Credit Transaction Act
FBI	Federal Bureau of Investigation
FERPA	Family Educational Rights and Privacy Act
FTC	Federal Trade Commission
GBLA	Gramm Leach Bliley Act
GDPR	General Data Protection Regulation

LIST OF ABBREVIATIONS

GPS	Global Positioning System
HIPAA	Health Information Portability and Accountability Act
ICO	Information Commissioner's Office
IDC	International Data Cooperation
IEE	Ethically Aligned Designed
IBM	International Business Machines Corporation
IoT	Internet of things
IoPTS	Internet of Things People and Services
ITI	Information Technology Industry
MIT	Ministry of Industry and, Information Technology
MLPS	Multi-Level Protection System
NSA	National Security Agency
OASIS	Open Archival Information System
OECD	Organization for Economic Co-operation and Development
RFID	Radio-frequency identification
R&D	Research and Development
RPM	Resale Price Maintenance

LIST OF ABBREVIATIONS

UDHR	Universal Declaration of Human Rights
UNCTAD	United Nations Conference on Trade and Development
UNIDIR	United Nations Institute for Disarmament Research
U.S.	United States

CHAPTER 1: INTRODUCTION

The right of privacy has deep roots in Anglo-American legal traditions. [1] Naturally, the right of privacy is said to have its origins in the common law. In his famous book, A *Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract* published in 1878, [2] Judge Thomas Cooley, in a classification of rights in the law of torts,[3] identified personal immunity as a right of complete immunity: to be let alone. In 1890, Samuel Warren and Louis Brandeis relied on Cooley's classification and crystalized the right of privacy as the right of an individual "to be let alone." [4]

Over a century later, the European Court of Justice in the case of *Google Spain v. Gonzalez*[5] adopted language similar to that of Judge Cooley by recognizing the right of privacy to include "the right to be forgotten." [6] In the U.S., the concepts of the rights of personal immunity and privacy characterized by Cooly and Warren and Brandeis found acceptance through codification in regulations and legislation.

[1] See Justices of the Peace Act 1361, 34 Edw. 3, c. 1. (Eng.) "First, That in every County of England shall be assigned for the keeping of the Peace, one Lord, and with him three or four of the most worthy in the County, with some learned in the Law, and they shall have Power to restrain the Offenders, Rioters, and all other Barators, and to pursue, arrest, take, and chastise them according their Trespass or Offence." See also early cases related to privacy in the Anglo-American early traditions, Gee v. Pritchard, 2 Swans. 402, 36 Eng. Rep. 670 (1818) (Related to publications of private letters) Prince Albert v. Strange, 2 De G. & Sm. 652, 41 Eng. Rep. 1171, 1 Mac. & G. 25, 64 Eng. Rep. 293 (1849) (The court conceded an injunction to Prince Albert do not have his catalogue etchings published by a stranger.)

[2] THOMAS M.COOLEY, A TREATISE ON THE LAW OF TORTS: OR THE WRONGS WHICH ARISE INDEPENDENTLY OF CONTRACT, (Callaghan, 14 ed., 1932).

[3] See William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 383-423 (1960) Prosser based on Samuel D. Warren and Louis D. Brandeis, article The Right to Privacy and several cases involving privacy. Divided tort privacy in four as follows 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness. Which was a legacy to the America law of privacy according to Neil Richards et al., see Prosser's *Privacy Law: A Mixed Legacy*, 98 Calif. L. Rev.1887-1924 (2010).

[4] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[5] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014 ECLI: EU: C: 2014:317 [hereinafter Google Spain SL v. AEPD].

[6] REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/43).

However, the right of privacy embodies a broader general principle of individual liberty vigorously advocated by moral philosophers in England[7] and eloquently expressed by Thomas Jefferson in the Declaration of Independence of the United States. [8] Liberty was one of the other *inherent* and *unalienable* rights[9] of man which consisted of the right to life, liberty, and the pursuit of happiness. The characterization of these rights as *inherent* and *unalienable* has certain significant implications.[10] They do not derive their existence from the government or legislation, but the obligation of government is to protect them. Thus, the right of privacy being part of the inherent and unalienable right of liberty is of extreme importance and enjoys elevated existence in the law.

So important was the right of privacy to the Framers of the United States Constitution that five of the first ten amendments[11] together with the fourteenth amendment[12] provided various

[7] See Glenn Negley, *Philosophical views on the Value of Privacy*, 31-319-325 (Spring, 1966), the author discusses the philosophical views of philosophers such as Hegel, Peter Laslett, Robert Owen and Bentham, concluding that "if privacy is defined as an essential requirement for the achievement of morality, then privacy is a right that the law must protect and provide."

[8] Declaration of Independence (U.S. 1776).

[9] Declaration of Independence (U.S. 1776).

[10] J. W. Cooke, Jefferson on Liberty, 34 Journal of the History of Ideas no.4 567(Oct-Dec. 1973).

[11] See U.S. Const. amend. I. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press."

U.S. Const. amend. III. "No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law."

U.S. Const. amend. IV. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.", see

U.S. Const. amend. V. "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

U.S. Const. amend. IX. "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

[12] U.S. Const. amend. XIV, § 1. "All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal

forms of privacy protection to individuals. It appears that while the right to privacy may trace its roots to the common law, the inherent nature of that right has led to its recognition and protection in modern constitutions, in the Universal Declaration of Human Rights,[13] the European Human Rights Convention,[14] and the Fundamental Rights Convention. [15] Privacy is a fundamental right that cannot be changed due to technological advances.[16] The concept of privacy, which involves personal information, does not change because of the way this information is collected and stored by modern technological devices.[17] Part of what is protected in privacy is personal information. What advances in modern technology facilitate is the gathering, storing, and manipulation of personal information as digital data formats. However, the changes in the format of the personal information collected by advanced technological methods does not deprive that information of privacy protections.[18]

While the nature and scope of privacy protections continue to be contested, the situation has been greatly complicated by the advancements made in modern technology, particularly

protection of the laws." See also, Exploring Constitutional Conflicts, *The Right of Privacy: The Issue: Does the Constitution protect the right of privacy? If so, what aspects of privacy receive protection?* http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (last visited Apr. 04.2020).
See the right of privacy discussed in Griswold v. Connecticut, 381 U.S. 479 (1965) (The United States Supreme Court held the right of privacy related to birth control inside a marriage.) See also Robert B. McKay, The Right of Privacy: Emanations and Intimations, 64 Mich. L. Rev.259-282 (Dec. 1965). The author discuss important cases related to privacy and how the court held the cases, pointed important dissents.

[13] G.A.Res.217 (12) A, Universal Declaration of Human Rights (Dec.10.1948). See Article 12 of the UDHR "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." See General Assembly resolution 68/167, *The right to privacy in the digital age,* A/RES/68/167 (18 December 2013), https://undocs.org/A/RES/68/167
See also the International Covenant on Civil Political Rights Article 17 "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.2. Everyone has the right to the protection of the law against such interference or attacks".

[14] REGULATION (EU) No 235/2014, 2014 O.J (L77/92).

[15] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.

[16] DOUGLAS MAULE ET AL., MEDIA LAW ESSENTIALS 119 (Edinburgh University Press, 2010).

[17] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, 6 (N.Y.U. Press, 2004).

[18] BRIAN W. KERNIGHAN, UNDERSTANDING THE DIGITAL WORLD: WHAT YOU NEED TO KNOW ABOUT COMPUTERS, THE INTERNET, PRIVACY, AND SECURITY, 3 (Princeton University Press 2017).

computer science and the use of artificial intelligence in areas that affect the daily lives of people. To guarantee the protection of life, fundamental rights, and liberty under national constitutions, conventions, treaties, and international humanitarian law, the governments of several countries have sought to ensure these rights through regulations including data protection instruments. The use of personal data by artificial intelligence for various purposes introduced new questions on the issue of the privacy protections, including what is guaranteed by constitutions and international conventions.[19]

Most of the time, data protection regulations generally face two problems. First, the governments must determine the constitution, content, and scope of data protection to ensure the full realization of the rights and freedoms guaranteed by law. Second, they must confront the constantly evolving and dynamic environment within which data protection is supposed to operate. Currently, one of the challenges covering data protection is the increased need for artificial intelligence (AI). Artificial intelligence "is the science and engineering of making intelligent machines, especially intelligent computer programs."[20] This new type of science and engineering of AI has rapidly complicated the task of any data protection regime since the input of data is what makes machine intelligence.

Technology has changed the ways humans act, react, and think. The permanent necessity to pursue, know, and see without physically visiting places facilitated the development of data.[21] People want comfort and easy lives. In other words, people want to buy, receive, and send things

[19] See J. David Bolter, *Artificial Intelligence*, 113 MIT Press 1 (summer, 1984), Bolter starts with the definition of Artificial intelligence made by Marvin Minsky, is "the science of making machines do things that would require intelligence if done by men." The author explains through examples, theories, and whether machines can think. See also BERNARD MARR ET AL., ARTIFICIAL INTELLIGENCE IN PRACTICE: HOW 50 SUCCESSFUL COMPANIES USED AI AND MACHINE LEARNING TO SOLVE PROBLEMS ch. 1 (Wiley, 2019) (eBook).

[20] John McCarthy, *What is AI? / Basic questions what is AI? / Basic questions,* http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html (last visited Dec.15, 2019).

[21] See *Id.* at 1.See also BRIDGETTE WESSELS ET. AL., OPEN DATA AND THE KNOWLEDGE SOCIETY 20 (Amsterdam University Press, 2017).

with a single click. It is difficult to imagine a world without technological tools. Everything consumers do is related to machinery, which makes life straightforward. Daniel Solove states, "The past few decades have witnessed a dramatic transformation in the way we shop, bank, and go about our daily business—changes that have resulted in an unprecedented proliferation of records and data."[22] All of these records of stored data are manipulated in a meaningful way, delivering information to corporations for several purposes, such as redesigning products, creating new products, and increasing sales.[23] Moreover, data storage processes started with the necessity of government to control society in several areas, such as immigration, criminal records, and others. However, the question is how safe is data, and how much of this data is being used for the prosperity of society? How can people protect their privacy in a technological world especially with AI? Do laws effectively safeguard people's privacy? In Alex Preston's words, "[W]hat is the personal and psychological impact of this loss of privacy? What legal protection is afforded to those wishing to defend themselves against intrusion? Is it too late to stem the tide now that scenes from science fiction have become part of the fabric of our everyday world?"[24] These questions are important to consider when dealing with individual lives. The amount of data generated is immense. It includes every single search or inquiry people perform when they use technological tools.[25] The pivotal point is whether governments and private companies should assure that all of these collected data are being used to improve human life. Nevertheless, the question remains whether information is being used to segregate or substitute the function of humans that can be

[22] SOLOVE, *supra* note 17, at 1.

[23] See DAVID STEPHENSON, BIG DATA DEMYSTIFIED: HOW TO USE BIG DATA AND DATA SCIENCE TO MAKE BETTER BUSINESS DECISIONS AND GAIN COMPETITIVE ADVANTAGE ch.1(FT Publishing International, 2018) (eBook).

[24] Alex Preston, *The Death of privacy Google knows what you're looking for. Facebook knows what you like. Sharing is the norm, and secrecy is out. But what is the psychological and cultural fallout from the end of privacy?*, the guardian (Aug.03.2014), https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

[25] See BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD, 7(W. W. Norton & Company, 2016).

harmful. In addition, it is not transparent what companies are doing with the data collected. In fact, society is facing a technological revolution. Andreas François Vermeulen describes this as the Fourth Industrial Revolution, "[S]tanding on the brink of a technological and social revolution that will fundamentally alter the way humans live, work, and relate to one another"[26] Undoubtedly, this revolution will not happen in the future, it is happening now. As an example, in the past, craftsmen were replaced with machines when the industrial revolution[27] took place. The new manufacturing process replaced the craftsman and the men became the operators of machines. After that, the Internet became the most powerful weapon that continues to collect data around the world. Computers, through programs and advanced software, have the ability to recognize faces, [28] drive cars,[29] play games,[30] control-manufacturing processes,[31] and perform other innumerable functions that are making society vulnerable. The world is experiencing AI, where a computer is capable of learning everything people spend their entire lives learning. For instance, machines, are able in a short amount of time to play a difficult game and come out with the same possibilities that humans

[26] ANDREAS FRANÇOIS VEMEULEN, INDUSTRIAL MACHINE LEARNING: USING ARTIFICIAL INTELLIGENCE AS A TRANSFORMATIONAL DISRUPTOR ch. 13 (Apress, 2019) (eBook). See also, PETER MORGAN, MACHINE LEARNING IS CHANGING THE RULES (O'Reilly Media, Inc. Jul.2018) (eBook).

[27] The Industrial Revolution was a period of major industrialization and innovation that took place during the late 1700s and early 1800s. The Industrial Revolution began in Great Britain and quickly spread throughout the world. James Chen, *Industrial Evolution, What was the Industrial Revolution?,* Investopedia (Updated Jul.5,2019). https://www.investopedia.com/terms/i/industrial-revolution.asp

[28] See Peter Trepp, *How Face Recognition Evolved Using Artificial Intelligence,* Facefirst (Jan.07.2020), https://www.facefirst.com/blog/how-face-recognition-evolved-using-artificial-intelligence/

[29] See NVIDIA, "POWERING SAFER, SMARTER CARS -Artificial Intelligence (AI) gives cars the ability to see, think, learn and navigate a nearly infinite range of driving scenarios. NVIDIA uses the power of AI and deep learning to deliver a breakthrough end-to-end solution for autonomous driving—from data collection, model training, and testing in simulation to the deployment of smart, safe, self-driving cars."
NVIDIA, Self-Driving Cars, Driving innovation: Building AI- Powered Self Drivers Cars, https://www.nvidia.com/en-us/self-driving-cars/ (last visited Apr.04.2020).

[30] See Nick Statt, *How Artificial Intelligence Will Revolutionize the Way Video Games Are Developed and Played: The advances of modern AI research could bring unprecedented benefits to game development*, (Mar.6.2019), https://www.theverge.com/2019/3/6/18222203/video-game-ai-future-procedural-generation-deep-learning

[31] See Philip Kushmaro, *5 ways industrial AI is revolutionizing manufacturing, In no other sector is artificial Intelligence having more of an impact than on manufacturing , and the revolution is just beginning*, (Sep.27.2018), https://www.cio.com/article/3309058/5-ways-industrial-ai-is-revolutionizing-manufacturing.html

take time to develop, such as AlphaGo Zero.[32] They also can reproduce the human voice, translate a text in several languages, and perform other tasks learned from experience generated through data processes. How to control this robust tool is a question that legislators, who are contending with this problem, need to answer. Unfortunately, the law often appears when there is a problem to solve. Some countries tried to predict the future by creating regulations. Nonetheless, when the real situation comes, legislators need to adapt or review the laws. Another pressing question is: Will governments and corporations be able to identify and regulate AI?

In 1983, while studying computer science as a doctoral student, Kai-Fu Lee observed that, "artificial intelligence is the elucidation of the human learning process, the qualification of the human thinking process, the explication of human behavior, and the understanding of what makes intelligence possible."[33] Thirty-seven years ago, it is possible that people potentially thought that Lee's statement was a hallucination of a clever young scientist. However, the perception remains almost the same today. It is unfathomable to think that a machine humans created can replace them, be faster, and solve problems in seconds. It seems to be a new super tool that nobody can stop. How is this powerful machine able to think like a human and how will this affect the current generation? Therefore, the purpose of this study is to research how data protection works in the ambiance of AI and how it affects the right "to be let alone,"[34] or in a modern world, the right "to be forgotten."[35] The nature and scope of AI tools also have significant implications in other areas

[32] See David Silver et al., *AlphaGo Zero: starting from scratch*, DeepMind (Oct.18.2017), https://deepmind.com/blog/article/alphago-zero-starting-scratch

[33] KAI-FU LEE, AI SUPER POWERS CHINA, SILICON VALLEY AND THE NEW WORLD ORDER 7 (Houghton Mifflin Harcourt Bos. N.Y.C. 2018).

[34] Warren and Brandeis, *supra* note 4.

[35] REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/43).

of law, such as intellectual property[36] and related areas of protection, including copyright,[37] patent,[38] trade secret,[39] trademark,[40] and competition law.[41] While the intellectual property issues raise interesting questions for research, they present a different set of inquiries for future endeavors. This thesis will, however, focus on the implications of AI innovations on data protection.

Moreover, to reach its purpose, this investigation seeks the answers to the following questions. What are the legal implications of AI for protecting data? How can the privacy of

[36] See, Jan Feuerhake, LL.M., AI, data protection and data ownership, https://iot.taylorwessing.com/ai-data-protection-and-data-ownership/ (last visited, Feb.07.2020).

[37] See, WIPO Paris Convention for the Protection of Industrial Property, https://wipolex.wipo.int/en/text/287556
MARSHALL A. LEAFFER, UNDERSTANDING COPYRIGHT LAW, 5 (Carolina Academic Press, 7 ed. 2019).
Kalin Hristov, *Artificial Intelligence and the Copyright Dilemma*, 57 IDEA: The IP L. Rev., no 3, 433 (2017).
Gerald Spinder, *Copyright Law and Artificial intelligence*, IIC 50, 1049 (Oct. 2019).
U.S. CONST. art. 1, § 8, cl. 8.
U.S. Copyright Law, *Copyright Law of the United States (tittle 17*), Copyright.gov (Dec. 2016).
Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S 340 (1991).
China IPR, *Copyright Protection in China A Guide for European SMEs*, (last update 2010).
Paul Sawers, *Chinese Court rules AI-Written article is protected by copyright*, VB (Jan. 10.2020), https://venturebeat.com/2020/01/10/chinese-court-rules-ai-written-article-is-protected-by-copyright/

[38] For information about patent regulations see STEPHEN M. MCJOHN, EXAMPLES & EXPLANATIONS INTELLECTUAL PROPERTY, 249 (6 Ed. 2019). See also TYLER T. OCHOA, ET AL., UNDERSTANDING INTELLECTUAL PROPERTY LAW (4 ed. 2020).
35 U.S.C.A §101 (2017).
See *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014).
See European Patent Office, Guidelines for Examination, https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm (last visited Feb. 19.2020).
John G. Flaim et al., *Subject-matter eligibility in the United States, Europe, Japan, China and Korea, WIPO Technology Trends 2019: Artificial Intelligence*. World Intellectual Property Organization, 96 (2019).
Patent Law of the People's Republic of China, article 22, http://english.sipo.gov.cn/lawpolicy/patentlawsregulations/915574.htm

[39] See KIRSTEN M. KOESPSEL, TRADE SECRETS: A LEGAL RESEARCH GUIDE, INTRODUCTION, WILLIAN S.HEIN & CO., INC. (2nd.ed 2019).
18 U.S.C.A. § 1839 (2018).
DIRECTIVE (EU) 2016/943, art.2, 2016 O.J. (L 157/1).
Laney Zhang, *China: Trade Secret Provisions under Anti-Unfair Competition Law Revised*, The Law Library of Congress, Legal Monitor (Jun.06.2019), https://bit.ly/2T6wV7t.

[40] CCPIT Patent & Trademark Law Office, *The Revised PRC Anti-Unfair Competition Law Took Effect on* April 23, 2019, IP News (Apr.26.2019), https://www.ccpit-patent.com.cn/node/6183

[41] E. THOMAS SULLIVAN ET AL., UNDERSTANDING ANTITRUST AND ITS ECONOMIC IMPLICATIONS, 3 (Carolina Academic Press, 7 ed. 2019).
Nathan Wilson, *Reduced Demand Uncertainty and the Sustainability of Collusion: How AI Could Affect Competition*, Federal Trade Commission, 2 (Jun.2019), https://bit.ly/3cKjOCe Artificial
Thomas A. Hemphill, *Artificial Intelligence and the Antitrust Challenges, Inside sources* (Aug.15,2019) https://www.insidesources.com/artificial-intelligence-and-the-antitrust-challenges/

individuals be affected by AI? How can data protection laws control the gathering of personal data? These are some of the questions that prompted this study. The protection of privacy has become a challenge in the digital era because AI tools raise new issues regarding the protection of personal data and the deterioration of privacy protection. It seems that with the emergence of modern technology, the "right to be let alone"[42] has extended to the "right to be forgotten."[43]

The justification for and the importance of studying this subject matter is the need for more protection and regulations to safeguard privacy. Indeed, privacy protection has been widely discussed, but not from the perspective of the implications of AI[44]. With the increasing use of personal data in the development of AI innovations, the focus on the implications of AI, which has been largely underexplored, is necessary. It is required since technological advances are accelerating process, governments and companies are trying to prevent problems through regulations and other alternatives. Scholars and professors who have contributed to the scholarship about technological advances are the inspiration for deepening the knowledge in this area. The goal of this contribution is to present another viewpoint. First, this thesis concentrates on beneficial regulations that can prevent society from being harmed by powerful machines or completely losing the "right to be let alone or forgotten." Second, it discusses the benefits AI can bring. The motivation to write this paper comes from curiosity, about data protection regulation work in the atmosphere of new technologies, and what laws would be suitable.

[42] Warren and Brandeis, *supra* note 4

[43] REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/43).

[44] AS EXAMPLES SEE, JAMES WALDO ET AL., ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE, 430 Nat'l Academies Press, (2007), discuss privacy and technology but not the direction relation with AI. See also DARRELL M. WEST, USING DIGITAL TECHNOLOGY TO FURTHER SOCIAL AND POLITICAL INNOVATION, 219 (Brookings Institution Press, 2011). The chapter ten of this book is devoted to safeguard privacy and security by explaining how vulnerable people's privacy are. See, ANDREW MCSTAY, PRIVACY AND THE MEDIA, 216 (Sage Publications, 2017). Approaches the nature of privacy and its relationship with modern media and networked communication. See TIANQING ZHU ET AL., DIFFERENTIAL PRIVACY AND APPLICATION, 235 (Spring, 2017).The authors explains some ways of data collection related to personal information differencing privacy and data publishing in many settings.

The methodology utilized in this study is qualitative bibliographic research, aggregating information from different archival studies and experts who study the issue and present distinct approaches in academic journals, books, e-books, magazines, and online resources as well as sites, organizations, and library catalogs. The materials were analyzed and compared to show agreements and disagreements about the subject. The analysis of these materials provided a review of what scholars have been investigating and writing with regard to data protection and how AI affects it. This methodology was pivotal in guiding the researcher to new conclusions and making contributions to the field. The method is inductive and analytic. The theoretical contributions are based on the ideas of Daniel Solove, Kai-Fu Lee, Stephen M. McJohn, and Bernard Marr, among other important authors who have studied this subject.

This investigation is divided into five parts. Chapter 1 introduces the topic. Chapter 2 is devoted, first, to tracing the history of AI and defining types of data, including how they are generated, and how AI and big data work together. Second, it addresses the definition of privacy, and the concept of privacy in the European Union (EU), China, and the United States (U.S.). Third, it provides a data protection definition, principles, requirements, and general data protection regulations, and outlines the approach of the China Cybersecurity Law of the People’s Republic of China (CSL) and the U.S. framework overview, focusing on the most complete law of data protection. Finally, it presents a comparative approach between regulation of AI and data protection in the three legal systems, concluding with a summary of the data protection laws. Chapter 3 addresses how global companies are dealing with data protection and potential AI risks, by focusing on Facebook, Google, and Amazon. This chapter also stresses AI and data ownership, and AI’s impact on society. The chapter concludes by presenting policy options for AI. In addition, it applies data protection principles and requirements applied to AI and discusses the scope of data protection regulation. Chapter 4 is committed to liability issues, privacy, security, and business. It also includes the legal requirements for automated decision-making, blockchain, regulations, and limitations to data transfers. Chapter 5 is dedicated to some concluding explanations.

CHAPTER 2: ARTIFICIAL INTELLIGENCE

The right "to be left alone"[45] and the protection of personal data is challenged by the emergence of artificial intelligence (AI). This means that privacy as a fundamental right is being disintegrated. When machines use personal data without limitations, they intrude privacy.

The Internet brought unimaginable technological advances and tools, such as Erica[46] from the Bank of America that provides financial feedback from bank accounts, and Alexa[47] from Amazon that suggests items to purchase. In many situations, people deal with aimless technological devices, which means they do not know if these devices bring benefits or put their privacy in danger.[48]

The balance between privacy and technology is becoming a puzzle, where humans are exchanging the right to privacy for commodities.[49] Imagine the following possibilities: the ability to unlock your cellphone with face-recognition, find advertisement promotions according to your thoughts, and know what you need to buy without opening your fridge or being at home. Further, imagine interacting with Siri (iPhone), requesting an Uber ride and knowing precisely when the driver will arrive through the Uber app, and so on.[50] These incredible modern everyday

[45] Warren and Brandeis, *supra* note 4.

[46] See Bank of America Newsroom, *Introducing Erica Insights: Bank of America's AI- Driven Virtual Financial* Assistant Just Got Smarter, (Oct.22,2018), https://newsroom.bankofamerica.com/press-releases/consumer-banking/introducing-ericar-insights-bank-americas-ai-driven-virtual

[47] See Amazon Alexa, *Alexa Science: Delivering Tomorrow's Vision for Conversational AI Today*, https://developer.amazon.com/pt-BR/alexa/science, (last visited Feb.21, 2020).

[48] CHRISTOPHER T. ANGLIM ET AL., PRIVACY RIGHTS IN THE DIGITAL AGE, xxi (Grey House Publishing, 2015) (eBook).

[49] See JOSEPH PHELPS ET AL., PRIVACY CONCERNS AND CONSUMER WILLINGNESS TO PROVIDE PERSONAL INFORMATION, 19 SAGE 27-41(Spring, 2000). The authors explain how consumers exchange personal information for commodities and some types of personal information, observe that the paper was wrote in 2000. Which shows that the concerns about privacy and technology has been subject of many scholars for many years.

[50] See HAOWEI LIU, FACE DETECTION AND RECOGNITION ON MOBILE DEVICES, MORGAN KAUFMANN (2014) (eBook), the author explain in details how face recognition works. See, Apple, *Use Siri on all your Apple devices*, Apple,

technologies are simple examples of AI. However, the question is how these technologies become part of a human's life. Can machines think? One of these questions comes from Alan M. Turing who in 1950 wrote an article reflecting on how machines can think. Alan explains that a game called Imitation Games "is played with three people: (A) a man, (B) a woman, and (C) an interrogator who may be of either sex. The interrogator stays in a room apart from the other two. The objective of the game is for the interrogator to determine which of the other two is the man, and which is the woman."[51] One of the players is a computer, and if the interrogator cannot determine which one is human, that means the computer is intelligent. Tom Taulli explains, "The genius of this concept is that there is no need to see if the machine actually knows something, is self-aware, or even if it is correct. Rather, the Turing Test indicates that a machine can process large amounts of information, interpret speech, and communicate with humans."[52] Hence, this was the first insight into machine thinking, which is where the concept of AI comes from.

Professor John McCarthy asserts that Artificial Intelligence (AI) "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."[53] It is the capability to make a machine perform the same functions as humans; the machine reproduces what a person takes a lot of time to learn.

https://support.apple.com/en-us/HT204389 (last visited Apr.09.2020). See also Uber, *How to use the Uber app*, Uber, https://www.uber.com/us/en/about/how-does-uber-work/ (last visited Apr.09.2020).

[51] Alan M. Turing, *Computing Machinery and Intelligence*, LIX Mind 433 (1950).

[52] TOM TAULLI, ARTIFICIAL INTELLIGENCE BASICS: A NON- TECHNICAL INTRODUCTION, ch. 1 (Apress, 2019) (eBook).

[53] John McCarthy, *What is AI? / Basic Questions* http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html (last visited 01/29/2020).

Before going into a modern concept of AI, it is necessary to present below the evolution of AI throughout the years by SAS Insights.

1950s–1970s
Neural Networks
Early work with neural networks stirs excitement for "thinking machines."

1980-2010s
Machine Learning
Machine learning becomes popular.

Present Day
Deep Learning
Deep learning breakthroughs drive AI boom.

Figure 1. Artificial intelligence revolution over the years.[54]

2.1 AI History.

The early work with neural networks started in 1956 when McCarthy at Dartmouth University organized a ten-week research project called, "A Study of Artificial Intelligence." The goal of the summer program was to put together a group of scientists to develop machines that could learn what humans do. Based on the assumption that the learning process can be precisely described, the ten-week research project was a crucial point in AI. Following developments from there, young academics started to exploit new ideas. For instance, the Logic Theorist program was

[54] SAS Insights Analytics Insights, *Artificial Intelligence What it is and why it matter,* https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html#close (last visited Jan 29, 2020). See Joanna Bristol a leading on AI ethics, she defines AI: "as intelligence that is an artefact. Intelligence is about moving from perception to action. It's being able to recognize context, generate some information and possibly some agency to change something in the world. And that is everywhere. Our thermostats are intelligent in that way." Fraser Myers, *AI: inhuman after all? Joanna Bristol on what the world gets wrong about robots and AI,* Spiked (Jun.14,2019), https://www.spiked-online.com/2019/06/14/ai-inhuman-after-all/

the creation of Hebert Simon working with Allen Newell and Cliff Shaw. The Logic Theorist program was designed to read more than numbers. Moreover, it is considered the first AI program developed. Subsequently, other programs and advances were gaining prominence. In the later 1950s, McCarthy did more than promote the founding of the MIT Artificial Intelligence Laboratory. He also developed other programs related to the programming language. In 1961, McCarthy drew up the idea of time-sharing, which developed the Internet and cloud computing.[55] Tom Taulli asserts,

> From 1956 to 1974, the AI field was one of the hottest spots in the tech world. A major catalyst was the rapid development of computer technologies. They went from being massive systems—based on vacuum tubes—to smaller systems run on integrated circuits that were much quicker and had more storage capacity.[56]

Thus, the first objectives of AI developers started to flourish through strong machines with programs directed to human capacities. An important incentive to these advanced programs and discoveries was the Federal Government's support and interest in promoting the industry to develop new technologies for specific achievements, such as the Apollo space program and other projects related to the Cold War. Between 1970 and 1980, AI was almost suspended because of economic crises and other issues that affected funds for developing the technology, called AI winter.[57] AI had some later advances and discoveries, and today is a leading innovation that has transformed the ways humans see the world. Geoffrey Hinton describes the modern concept of AI in the following terms:

> Modern AI is modeled after ideas about how the brain works. The way the brain works is, you have a big network of brain cells, an input comes in and stuff goes on and then you get an output and the output you get depends on the connection strengths between the brain cells. If you change those connection strengths you change the output you will get for each input.

[55] TAULLI, *supra* note 52.
[56] *Id.*
[57] *Id.*

> The way AI now works is instead of programming the computer you show it lots of examples it changes the connection strengths and it learns to produce the right answers without you ever programming.[58]

So, when Geoffrey affirms that a machine can learn from examples instead of being programmed, it means that AI is also a process gathered through deep learning. Kai-Fu Lee states, "Deep learning is what's known as 'narrow AI'- intelligence that takes data from one specific domain and applies it to optimizing one specific outcome. While impressive, it is still a far cry from 'general AI', the all-purpose technology that can do everything a human can."[59] Therefore, deep learning is one way to train machines to do what humans do through several examples and situations related to one area or subject matter. Perhaps this can be compared to the way humans learn, which is through examples, studying, reading, and listening; and, after all this, the learning process is finished. The machine learning process is similar to the human learning process.

In machine learning, many images that sometimes have human faces are provided to AI. In this training process, the computer creates its algorithm, which is known as unsupervised machine learning when the machine does not have someone guiding the process. This process can also happen with human supervision, which is known as supervised or semi-supervised machine learning. Deep machine learning is the process whereby the machine uses several layers of the artificial neural network to learn from training data.[60]

Scientists studying human brain behavior found a way not to program, but rather, train machines the same way human minds work. David Stephenson gives some examples of how AI works through different apps:

[58] Andrew Arruda, *Defining Artificial Intelligence with AI pioneers Bengio, Hinton, Ovbiagele & P M Tradeau* (Nov. 2017), https://blog.rossintelligence.com/post/ai-pioneers-bengio-hinton-ovbiagele-pm-trudeau.
[59] LEE, *supra* note 33, at 10.
[60] BERNARD MARR ET AL., ARTIFICIAL INTELLIGENCE IN PRACTICE: HOW 50 SUCCESSFUL COMPANIES USED AI AND MACHINE LEARNING TO SOLVE PROBLEMS ch. 1 (Wiley, 2019) (eBook).

> We interact with AI in Apple's Siri, Amazon's Echo, self-driving cars, online chat-bots and gaming opponents. AI also helps in less obvious ways. It is filtering spam from our inboxes, correcting our spelling mistakes, and deciding what posts appear on top of our social media feeds. AI has a broad range of applications, including image recognition, natural language processing, medical diagnosis, robotic movements, fraud detection and much more.[61]

Indeed, AI converts complex tasks into practical tasks that are easier to manage. The examples Stephenson cites above are just a few examples of AI exploitations in business, medicine, and everyday life.

Another significant concept is artificial general intelligence (AGI). Martin Ford says it "refers to a true thinking machine. AGI is typically considered to be more or less synonymous with the terms HUMAN-LEVEL AI or STRONG AI."[62] In simple terms, machines can make decisions without human interference, and develop solutions similar to and more quickly than humans.

2.2 Data Definition

A comprehension of the concept of data and how information is gathered will help the reader understand how data is AI fuel. Merriam Webster's Dictionary defines data as "information in digital form that can be transmitted or processed."[63] According to Cambridge Dictionary, "data is information, especially facts or numbers, collected to be examined and considered to help decision-making or information in an electronic form that can be stored and used by a computer."[64] Moreover, for the Reference Model for an Open Archival Information System (OASIS), data is "a

[61] STEPHENSON, *supra* note 23.

[62] MARTIN FORD, ARCHITECTS OF INTELLIGENCE: THE TRUTH ABOUT AI FROM THE PEOPLE BUILDING IT, ch.1 (Packt Publishing, 2018).

[63] Dictionary, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/dictionary (last visited Dec 15, 2019).

[64] Dictionary, CAMBRIDGE, https://dictionary.cambridge.org/dictionary/english/ (last visited Dec 15, 2019).

reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing. Examples of data include a sequence of bits, a table of numbers, the characters on a page, the recording of sounds made by a person speaking, or a moon rock specimen."[65] For this reason, in digital terms, data is all information that people can collect and store. It is crucial to understand how society uses and generates this data to discern how companies and governments manage it. Bridgette Wessels et al. state, "Data is pervasive and is used in all aspects of social life. It is collected, coded, interpreted, and used across a range of social practices, which are shaped by the production and consumption patterns of particular social contexts and sectors."[66] As a result, to perceive data requires also interpreting the existing types of data, keeping in mind that each society will generate several different types of data based on political, cultural, and organizational aspects. Hence, the objective here is to explain some of the most important types of data and how they work, keeping in mind that data is essential matter for modern society.

2.3 Types of Data

In the digital era, the combination of data and other information is what makes machines intelligent.[67] Thus, discerning how the process occurs through types of existent data is essential to understanding the way AI works. The first type of data is personal data, and from the name, it is possible to construe a definition. Personal data is every single data that identifies and relates to an individual. That means, if data cannot identify an individual, it is not personal data. Daniel J.

[65] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, RECOMMENDATION FOR SPACE DATA SYSTEM PRACTICES – REFERENCE MODEL FOR AN OPEN ARCHIVAL INFORMATION SYSTEM (OASIS) 10 (Magenta Book June 2012), https://public.ccsds.org/pubs/650x0m2.pdf

[66] BRIDGETTE WESSELS ET. AL., OPEN DATA AND THE KNOWLEDGE SOCIETY 26 (Amsterdam University Press, 2017).

[67] Willem Sundblad, *Data Is The Foundation For Artificial Intelligence and Machine Learning*, Forbes (Oct. 18.2018),https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/#a18ff4f51b49

Solove asserts, "In the Information Age, personal data is being combined to create a digital biography about us."[68] This is not a definition of data, but it gives the sense that personal data is the biography of someone. From this data, it is possible to know the name, age, sex, and address of a person, as well as other private personal information, what is known as sensitive data.

The second type of data is big data. It is a common term; however, people outside of the technology community have some difficulty defining it. According to David Stephenson, "The term 'big data' refers to a new class of data: vast, rapidly accumulating quantities, which often do not fit a traditional structure."[69] Jean Louis Monino asserts, "When the amount of data that an organization has to manage reaches a critical volume that requires new technological approaches in terms of storage, processing, and usage. Volume, speed, and variety are usually the three criteria used to qualify a database as big data'." [70] The term big data also means a huge amount of data. However, to understand whether this amount of information is useful, one needs to understand where big data comes from. Stephenson states that in the past, "We were frugal with storage, but the data we stored was small enough to manage."[71] The author explains that since the digital era started, people began saving data, such as pictures, movies, and small types of documents because the capacity to store was limited. Anyhow, with a faster advance of technology, the process of data creation has become easier. Due to this, the amount of data that can be stored is huge, and the creation of new technology facilitates the generation of more data. Stephenson asserts the following:

[68] SOLOVE, *supra* note 17, at 44.
[69] STEPHENSON, *supra* note 23.
[70] JEAN-LOUIS MONINO ET AL. BIG DATA, OPEN DATA AND DATA DEVELOPMENT, Key Concepts (Iste, 2016) (eBook).
[71] STEPHENSON, *supra* note 23.

> The *coup de grâce* came with the development of crowd-sourced digital publishing, such as YouTube[72] and Facebook[73], which opened the portal for anyone with a connected digital device to make nearly unlimited contributions to the world's data stores.[74]

Furthermore, this unlimited data becomes immensurable and the Internet has been playing an important role in this field. It seems as though humans developed a machine capable of recording and storing all the things they do. The Internet has become the most powerful tool that teaches through online courses, homemade videos, books, magazines, and other imaginable materials. In the digital era, everything is stored in computers and convertible in data. Notwithstanding this, computer experts started to manage the amount of information by creating supercomputers to solve problems. However, computer experts did not explore big data at all.[75] Consequently, in the twenty-first century, according to Stephenson, "There were several key developments towards the start of the twenty-first century. One of the most significant originated in Google. Created to navigate the overwhelming data on the newly minted world wide web, Google was all about big data."[76] Thus, companies started to think about how to manage, use, and store these immense amounts of data generated each second around the world. Big data is important because

> when you combine big data with high-powered analytics, you can accomplish business-related tasks such as: determining root causes of failures, issues and defects in near-real time, generating coupons at the point of sale based on the customer's buying habits, recalculating entire risk portfolios in minutes, detecting fraudulent behavior before it affects your organization.[77]

[72] YouTube is a free video sharing website that makes it easy to watch online videos. YouTube- What is YouTube https://edu.gcfglobal.org/en/youtube/what-is-youtube/1/ (last visited Dec. 21, 2019).

[73] The Facebook Company builds technologies that give people the power to connect with friends and family, find communities and grow businesses. https://about.fb.com/ (last visited Dec.21, 2019).

[74] STEPHENSON, *supra* note 23.

[75] See *supra id.*

[76] STEPHENSON, *supra* note 23.

[77] SAS INSIGHTS, Why is Big data important?, https://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited Dec.21, 2019).

As a result, big data becomes essential for companies to achieve success in understanding customer behavior through the digital information generated in each search, post, or purchase.

The third type of data includes structured, unstructured, and semi-structured data. Bernard Marr defines structured data as "[i]nformation that has a predefined data model or is organized in a predetermined way."[78] This type of data is specific and defined according to companies' purposes, such as clients' names, cellphone numbers, addresses, and last products bought. The business manager will decide which type of structured data is important to store for future marketing actions. On the other hand, unstructured and semi-structured data are all data generated without a predefined data model, which can be found in texts, images, or numbers. According to Bernard Marr, because of the variety of data people can generate, it is difficult to interpret this type of data because of the inconsistency of data collected. Thus, the use of traditional computer programs to analyze this type of data can be a challenge. In addition, the author provides an example to clarify semi-structured and unstructured data: "In semi-structured data, tags or other types of markers are used to identify certain elements within the data, but the data doesn't have a rigid structure. For example, a Facebook post can be categorized by author, data, length, and even sentiment but the content is generally unstructured."[79] Companies can use this type of data when analyzing different tasks.

The next type is internal data. This is all information that corporations collect and keep for individual business goals. Bernard Marr cites the following examples: "customer feedback, sales data, employee or customer survey data."[80] These data are important for the company to redesign products, send promotions, and track clients' desires. Another interesting type of data is external

[78] BERNARD MARR, BIG DATA: USING SMART BIG DATA, ANALYTICS AND METRICS TO MAKE BETTER DECISIONS AND IMPROVE PERFORMANCE, ch.3 (Wiley, 2015) (eBook).

[79] MARR, *supra* note 78.

[80] *Id*. at ch.1

data, which can be defined from the name. External data is all data generated from a third party that needs authorization to be accessed. This type of data can be private or public. Marr states,

> Public data is data that anyone can obtain – either by collecting it for free, paying a third party for it or getting a third party to collect it for you. Private data is usually something you would need to source and pay for from another business or third party data supplier.[81]

Consequently, external data is used for several purposes, such as prospective clients, market values location, and new markets to exploit.

In the past, the types of data cited above were the most significant for the technological world. However, with the Internet, everything humans do through a computer leaves some trace.[82] Bernard Marr defines this new period as, "The world is being 'datafied' and there are now many forms of useful data. Some of the data forms are new such as social media posts; others have been around for a long time."[83] Therefore, it is extremely important to understand some of these new data types, and how they affect data processes is the main purpose of this paper.

All technology devices can record human decisions, and that means humans are being watched twenty-four hours a day, generating an immeasurable amount of activity data.[84] This activity data is recorded each time a person goes to a website to buy, search, and pay. Furthermore, nowadays, people also use the Internet to read online books, since the digital world has everything available.

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] See GEORGE ORWELL 1984, 256(Otbebookpublishing, 2020). The book is a classic novel about Winston Smith and his life in a city where the police force does a twenty for hour surveillance. Thus, through posters in many public places, the police force reminds the population they are watching them. The phrase in the post says "Big Brother is watching you." Which is applicable to the current life in society. Through technology people are been monitored twenty-four hours a day.

Bernard Marr explains:

> When we use an e-reader we are usually not just reading a digital image of the page – the text is datafied. That means that we can change font size, add notes, highlight text or search the book. This datafication also means that data is gathered about what we read, how long we read for, whether we skip pages, what pages we annotate and what we choose to highlight.[85]

Thus, technological devices are recording everything someone does through the Internet. Furthermore, enterprises are using all this data to create new products and improve existing ones.

The next data type is sensor data, which is generated from sensors. Bernard Marr approaches this type of data with a question: "Have you ever wondered that makes your smart phone (or smart anything for that matter) smart?"[86] With this question, the author invites the reader to reflect on how many sensors are in a smart phone as an example. Sensors can be found in the Global Positioning System (GPS),[87] which helps people find locations, calculate distance, and travel to different places without getting lost. There are several types of sensors that generate extensive data for different intents. The Internet of things (IoT)[88] is an example of how sensors are everywhere enabling communication in distinct ways.[89]

Open data is also an important concept. According to Jean Monino et al., "This term refers to the principle according to which public data (gathered, maintained and used by government

[85] MARR, *supra* note 78, at ch.1.

[86] *Id.*

[87] "The Global Positioning System (GPS) is a U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services." Official U.S. Government about the Global Positioning System (GPS) and related topics, *what is GPS?*, https://www.gps.gov/systems/gps/ (last visited Dec.21, 2019).

[88] The International Data Cooperation (IDC), defines Internet of Things (IoT) as a network of networks aggregating and interacting uniquely identifiable endpoints (or "things") that communicate autonomously using IP connectivity, whether locally or globally (The IoT is made up of technology-based connected solutions that allow businesses, organizations, and consumers to gain insights that help transform how they engage with the physical world of objects found in life and business.)
IDC Analyze the Future, Taxonomy, IDC'S Worldwide Semiannual Internet of Things Spending Guide Taxonomy, 2017; Update https://www.ibm.com/downloads/cas/56ZMODLB (last visited Dec.21, 2019).

[89] MARR, *supra* note 78 at ch.1.

bodies) should be made available to be accessed and reused by citizens and companies."[90] So, open data is all data collected by governments and private institutions, and the combination of all this data helps to advance technology and understand society's needs. The Open Knowledge Foundation[91] prescribes open data as "data that can be freely used, re-used and redistributed by anyone subject only, at most, to the requirement to attribute and sharealike."[92]

In addition, the organization states that the possibility to inter-operate, associate, and embody the different datasets is the key to developing better products and services. Some of the areas that have benefited from the use of open data are "innovation, impact measurement of policies, new knowledge from combined data sources and patterns in large data volumes."[93] Thus, open data is an important available resource for exploitation, which is playing a decisive role in technological premises, scientific research, and private companies. In conclusion, Jean-Monino et al., state:

> Furthermore, one of the main advantages associated with Open Data is that it promotes the development of a culture centered on information sharing and on cross-sector collaboration. As a cross-sector principle, Open Data can generate benefits for the economic, cultural and social spheres. The possible benefits that stem from such opening of data can, therefore, be exponential.[94]

Consequently, the association between this type of data and the others explained above are crucial to understanding how technology is driving the world and what is next.

Another new concept of data is Data Intelligence, defined by The International Data Cooperation (IDC) as "leverages business, technical, relational and operational metadata to provide transparency of data profiles, classification, quality, location, lineage, and context; Enabling

[90] MONINO ET AL. *supra* note 70, at ch. 2.

[91] Open Knowledge Foundation is a global non-profit organization focused on realizing open data's value to society by helping civil society groups access and use data to take action on social problems. Open Knowledge Foundation, *About*, https://okfn.org/about/ (last visited Dec.21, 2019).

[92] Open Knowledge Foundation, *Open Data Handbook* , 2009, http://opendatahandbook.org/guide/en/what-is-open-data/

[93] *Id.*

[94] MONINO ET AL. *supra* note 70, at ch. 2.

people, processes, and technology with trustworthy and reliable data."[95] This type of data helps organizations classify the data, such as where the data comes from, the last update, and how to use the data.

The types of data presented above are not an extensive list; however, they are the most relevant types of data to acquire some knowledge to understand the big picture. Therefore, the simplest concept to keep in mind is that data is everything people do when using technological tools to access the Internet, including using search engines, sending e-mails, buying goods, and so on.

2.4 AI and Big Data

AI and big data are the perfect combinations of machine learning. Stephenson states that "big data gave an even greater boost to AI with two key developments: we started amassing huge amounts of data that could be used for machine learning. We created software that would allow normal computers to work together with the power of a super-computer."[96] In this way, machine training was possible through the huge amount of everyday data that was generated for purposes such as Siri, Tesla, and Netflix,[97] which used different data features to achieve goals. The machine learning process is similar to the human brain; the quantity of training is important to make things perfect. Exposure to big data makes the program accurate.

[95] Steward Bond, *Defining Data intelligence : Intelligence about Data*, Not from Data, Nov.25,2019, https://blogs.idc.com/2019/11/25/defining-data-intelligence-intelligence-about-data-not-from-data/

[96] STEPHENSON, *supra* note 23, at ch.2.

[97] The following citations shows how this companies are using the data they collects. See Michael Simon, *Apple's Siri 'eavesdropping' controversy can be fixed with a toggle that should've been there all along,* Macworld (Jul. 29.2019). https://www.macworld.com/article/3411992/apple-siri-eavesdropping-controversy-privacy-toggle.html
See also, Danielle Muoio, *An ex-Tesla exec reveals how the company is transforming itself into a data powerhouse* (Jun. 26.2017), https://www.businessinsider.com/tesla-chris-lattner-explains-how-car-data-is-used-2017-6.
See Netflix research, *About*, https://research.netflix.com/research-area/analytics, (last visited Apr.09.2020).

Stephenson alleges,

> The quantity of training data and the technologies developed to process big data have together breathed new life into the field of artificial intelligence, enabling computers to win at *Jeopardy* (IBM's Watson computer), master very complicated games (DeepMind's AlphaGo) and recognize human speech better than professional transcriptionists (Microsoft Research).[98]

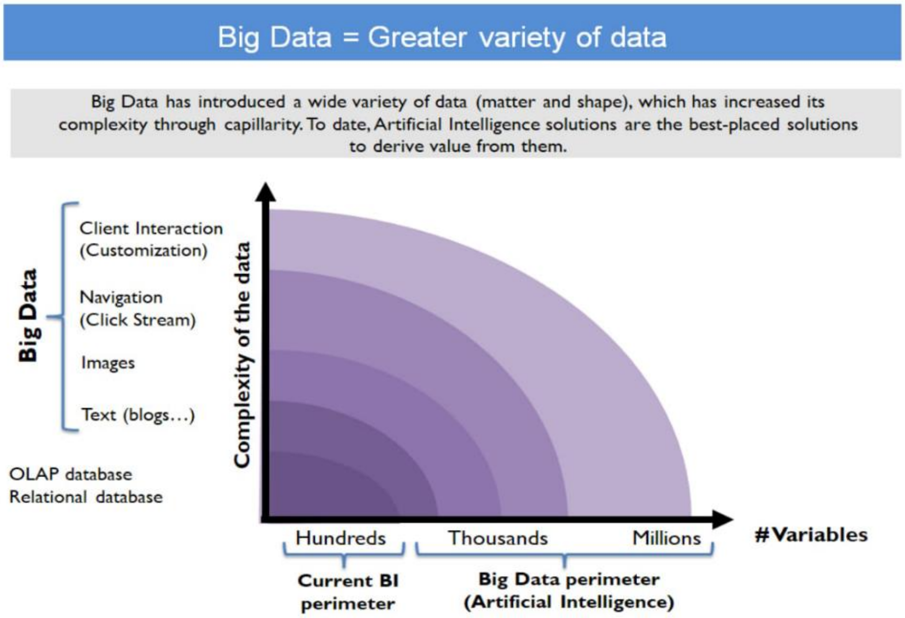
This means big data is the key element in machine learning. It is available everywhere because most of the activities in which people engage electronic devices generate data. Notwithstanding, corporations need to manage an immense amount of data generated everywhere, and the use of some techniques is essential to extract specific pieces of information. One of these techniques is known as data mining, and "data mining represents a set of discoveries of new structures in large data sets which involve statistical methods, artificial intelligence and database management."[99] Thereby, AI depends on data mining to learn and execute tasks, since through the data mining process, data is divided and organized. Monino et al. assert,

> Data mining is a technology that creates value and extracts information and knowledge from data. The development of this technology is the result of an increase in digital data which, relative to their abundance, is underexploited without the proper tools and expertise. This technology is based on a variety of techniques (artificial intelligence, statistics, information theories, databases, etc.) that require diverse skills at a high level.[100]

Consequently, data mining plays an important role in AI machine learning. Without this process, the value of big data cannot be fully explored.

[98] STEPHENSON, *supra* note 23, at ch.2.
[99] MONINO ET AL. *supra* note 70, at ch.3.
[100] *Id.*

The following illustration depicts how big data is an essential part of the machine learning process.



Big Data = Greater variety of data

Big Data has introduced a wide variety of data (matter and shape), which has increased its complexity through capillarity. To date, Artificial Intelligence solutions are the best-placed solutions to derive value from them.

Figure 2. Artificial intelligence and big data[101]

After providing an overview of the types of data, where they can be found, their definitions, and how they underline how AI works, it is of paramount importance to connect the compilation of personal data to AI purposes. When AI collects an immense amount of data and stores it, this data can have personal information such as a person's name, address, age, social security number, consumer preference, and so on. The act of storing this type of data should make companies responsible for any breach or misuse of the information in the sense that corporations would become more cautious when they use it.[102] Consider a second hypothetical situation where massive

[101] FERNANDO IAFRATE, ARTIFICIAL INTELLIGENCE AND BIG DATA: THE BIRTH OF A NEW INTELLIGENCE, 44 (ISTE, 2018) (eBook).

[102] See Benjamin Cheatham et al., *Confronting the risks of artificial intelligence*, McKinsey Quarterly (Apr.2019), https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence

amounts of personal data may be collected but also sanitized, to withdraw personal identifiable information. It is not an effective way to safeguard individuals' privacy because the data will be separated not related to a person, but a group[103]. For instance, a group of women with a certain age, living in state X, will soon have a health condition related to their habits. It could be used to increase insurance prices for this group. Thus, the fact that data is sanitized does not mean the data does not need protection, especially when taking into consideration that it can be used to target and discriminate against social groups.[104] Although a big portion of society worries about personal data, such as names, zip codes, education levels, and bank information, the absence of this data still leaves room for bias and risks to have decisions made based on these pieces of information, which can produce prejudice. Furthermore, to be targeted in a certain group without permission is a clear intrusion and also interferes with the right to be forgotten as long as the data can identify a race, group, or gender.

2.5 Privacy Definition

The pervasive collection of data for different AI innovation purposes makes the definition of privacy complicated. The “right to be let alone” has been interpreted in so many ways that privacy can have several different meanings. Jan Holvast asserts, “Data is a collection of details

[103] See Latanya Sweeney, *k-anonymity: A model for Protecting Privacy*. 10 Int. J. Uncertain. Fuzziness Knowl.-Based Syst., 558 (2002). In this article, the author explains that, the fact some companies managing personal data on removing specific identifiers such as name, address and telephone the data becomes anonymous. However, the author demonstrates that the process of re-identify individuals can be done by using remaining data. Other important point Sweeney states is that, there are other ways to identify a fraction of groups from their zip code, data of birth, and gender. Thus, this data should not be considered anonymous.

[104] See Ninghui Li et al., *Differential Privacy From theory to Practice*, 4 (Morgan & Claypool 2017). Through the lessons from privacy incidents it was possible to create the hypothetical situations where the data considered anonymous can be sufficient to identify individuals or groups. The authors suggest that this type of data should be protected and considered sensitive data.

or facts which, as such, are meaningless; however, when those details or facts are placed in a context which makes data usable, serious information can be gleaned. Depending upon the placement-context, the same data can be transformed into different information."[105] This puts the right to be let alone in a vulnerable position, since the control of privacy is in the hands of third parties.

When people started to live in communities and eventually formed cities, the necessity of privacy protection existed. However, with technological advances, the necessity to protect personal life intensified. How to keep privacy safe was a question raised in many cases in the years of 1741, 1820, and 1849 in England.[106] "The right to be let alone"[107] was a famous phrase in a treatise on torts, formulated by Judge Thomas Cooley. In 1890, Warren and Brandeis used this memorable quote to write a recognized publication about the right to privacy, which supported the development of privacy law in the United States. In the article, the authors claimed the following:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone' instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.[108]

[105] Jan Holvast, *History of Privacy*, Holvast & Partner, Privacy Consultants , NL- Landsmeer, The Netherland, https://link.springer.com/content/pdf/10.1007/978-3-642-03315-5_2.pdf , (last visited, Mar.17.2020).

[106] See Justices of the Peace Act 1361, 34 Edw. 3, c. 1. (Eng.) "First, That in every County of England shall be assigned for the keeping of the Peace, one Lord, and with him three or four of the most worthy in the County, with some learned in the Law, and they shall have Power to restrain the Offenders, Rioters, and all other Barators, and to pursue, arrest, take, and chastise them according their Trespass or Offence." See also early cases related to privacy in the Anglo-American early traditions, Gee v. Pritchard, 2 Swans. 402, 36 Eng. Rep. 670 (1818) (Related to publications of private letters) Prince Albert v. Strange, 2 De G. & Sm. 652, 41 Eng. Rep. 1171, 1 Mac. & G. 25, 64 Eng. Rep. 293 (1849) (The court conceded an injunction to Prince Albert do not have his catalogue etchings published by a stranger.)

[107] THOMAS C. COOLEY, LAW OF TORTS 29 (2d ed. 1888).

[108] Warren and Brandeis, *supra* note 4.

This article provoked discussions around the world about privacy. Thus, it was a fundamental document to develop laws to protect the privacy and the nature of human beings. Also in 1948, the Universal Declaration of Human Rights[109] (UDHR), Article 12 stated "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[110]

Notwithstanding, 279 years after the first cases about violations of privacy, governments around the world are still dealing with privacy law issues because as stated by Warren and Brandeis,

> The individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define a new the exact nature and extent of such protection.[111]

Therefore, the exact nature and extent of privacy protection will vary from time to time. It is not fixed in time. Hence, with technological advances, the creation of new regulations to safeguard privacy is vital.

2.5.1 The EU Privacy Definition.

The EU defines privacy as a human right in the Charter of Fundamental Rights of European Union Article 7 as follows: "Respect for private and family life- Everyone has the right to respect for his

[109] The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected and it has been translated into over 500 languages.
United Nations- *Shaping our Future Together* – Universal Declaration of Human Rights https://www.un.org/en/universal-declaration-human-rights/ (last visited Dec.26, 2019).

[110] G.A.Res.217 (12) A, Universal Declaration of Human Rights (Dec.10.1948).

[111] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

or her private and family life, home and communications."[112] Indeed, privacy is important and a very sensitive area for the EU Commission. The Commission understands that the power of privacy needs to remain in people's hands, so they need to determine when information should or not be used or disclosed. The Commission, through the definition of privacy as a human right, sought to provide the most important and strict concept of privacy. This definition delivered to states' member citizens the right to exercise the right to be let alone. The gathering of private information falls within a lack of respect because consumers do not know when information is stored, sold, or exchanged with other companies for different purposes without permission. The recognition of privacy as a fundamental right creates limitations to the collection of personal information, which provides safety to society.

2.5.2 China's Privacy Definition.

According to Hao Wang in China, "Although it is very difficult to define privacy accurately, privacy is still a significant value that underpins other fundamental rights. Chinese citizens' privacy should be free from interference from others."[113] Therefore, it appears that, in China, privacy is related to social values that a person is also responsible for protecting herself from intrusion. On the other hand, with the spread of technology and data collection, China is also facing different challenges to the right of privacy. It seems that the combination of data gathering and technology has endangered the ways a person can protect herself from interference. Lü Yao-

[112] Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[113] HAO WANG, PROTECTING PRIVACY IN CHINA, A RESEARCH ON CHINA'S PRIVACY STANDARDS AND THE POSSIBILITY OF ESTABLISHMENT THE RIGHT TO PRIVACY AND THE INFORMATION PRIVACY PROTECTION LEGISLATION IN MODERN CHINA 9 (Springer 2011).

Huai affirms this in the following statement: "The diverse conceptions of 'privacy' among contemporary Chinese citizens are by all means reflected in the law. In fact, even though up until now, Chinese law has not clearly defined privacy as a kind of independent right – the legal protection of privacy rights has gradually increased since the 1980s."[114] As a result, the Chinese Constitution in Chapter 2 addresses The Fundamental Rights and Duties of Citizens in Articles 37 to 40. They establish privacy protection through freedom of the person, freedom from insult, inviolability of the home, and private correspondence.[115] Moreover, the country also protects privacy through general principles of civil law and other documents that oversee privacy in different sectors, such as the law on the protection of minors, the law of protection of rights and interests of women, the law on lawyers, and so on.[116] On the other hand, dealing with constant privacy issues in 2016, China enacted the cybersecurity law (CSL) to protect privacy through data. This specific law will be discussed in 2.6.2.

2.5.3 The U.S. Privacy Definition

The concept of privacy in the United States varies according to the area of application. Daniel J. Solove et al. defend the idea that "the meaning of privacy depends upon the context, that there is no common denominator to all things we refer to as 'privacy.'"[117] The definition of privacy

[114] Lü Yao-Huai, *Privacy and data privacy issues in contemporary China, Chinese concept of privacy* 9 (Springer 2005).

[115] China, *Constitution of the People's Republic of China*, 4 December 1982, refworld, https://www.refworld.org/docid/4c31ea082.html (last visited Mar. 18. 2020)

[116] Lü Yao-Huai, *Privacy and data privacy issues in contemporary China*, *Chinese concept of privacy* 9 (Springer 2005). See also, MWE Law Offices and Practical Law China, *Data Privacy in China*, Thomson Reuters https://tmsnrt.rs/38Y9W4w , (last visited Mar. 18. 2020).

[117] DANIEL J. SOLOVE ET.AL, INFORMATION PRIVACY LAW 51 (N. Y. ASPEN Publishers, 2d Ed. 2006).

will vary from society to society because the elucidation of the term also includes some social values. Alan Westin defines privacy as,

> The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solicitude or small-group intimacy or when among larger groups, in a condition of anonymity or reserve.[118]

According to the author, the power to manage privacy should prevail in the individual's hands. The person should determine which information is personal and when the disclosure of this information is an intrusion to his/her privacy. This means privacy should be determined by individuals.

Although, the U.S. privacy definition can be found in different federal and state laws. The U.S. Constitution through the amendments guarantees the right to personal autonomy, which complements what Alan Westin stated above. The Constitution protects privacy beliefs through the First Amendment[119]. The Third Amendment[120] protects the privacy of the home, against soldiers' intrusion. The Fourth Amendment[121] protects privacy giving the right to people not to have their house unreasonable searched. Then the Fifth Amendment[122] protects private information

[118] ALAN F. WESTIN, PRIVACY AND FREEDOM 7(Atheneum Press N.Y.1967).

[119] U.S. Const. amend. I. "Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press."

[120] U.S. Const. amend. III. "Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press."

[121] U.S. Const. amend. IV. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[122] U.S. Const. amend. V. "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

against self-incrimination. The Ninth Amendment[123] opens the door to the protection of privacy in areas that the Constitution does not enumerate. However, the Fourteen Amendment[124] protects privacy and other rights through the due process clause.[125]

In conclusion, besides the overview of privacy definition in the three legal systems, this study also focuses on the following question. How to safeguard privacy with the proliferation of data? In the modern world, information about people is available through the Internet. Each time one searches, click on a website, post pictures, or thoughts on social media their privacy and personal data are shared.

Solove et al. argue that:

> Privacy involves the ability to avoid the powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan.[126]

The new technology is calling for the establishment of new protections. Governments and private companies have access to massive amounts of data that have personal information. However, can an individual protect himself? Are there boundaries?

Cristopher T. Anglim et at. assert:

> The advent of the digital age has created unprecedented opportunities to share and access information about each one of us. This makes it simpler and quicker than ever to obtain a store credit card, to pay bills online without ever writing a check, and to publish our ideas and thoughts to the world. But it also gives both government and the private sector unprecedented opportunities to keep an eye on

[123] U.S. Const. amend. IX. "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."
[124] U.S. Const. amend. IVX, § 1"All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."
[125] See *Griswold v. Connecticut*, 381 U.S. 479 (1965). This case upheld marital privacy.
See *Stanley v. Georgia*, 394 U.S. 557, 89 (1969). In 1969 the court ruled that a person in his own house has the right to see and possess pornography.
See *Roe v. Wade* 410 U.S. 113, 93 (1973). The Supreme Court held that the abortion was within the scope of the personal liberty, according to the Fourteen Amendment due process clause.
[126] SOLOVE ET AL., *supra* note 117, at 51.

> our movements, our interactions with others, and in some ways, our thoughts and ideas.[127]

In this way, the meaning of privacy makes it clear that protecting privacy is the biggest problem our society is facing. To prove that the variations of the meaning of privacy directly impact regulations, the general concepts of privacy in the EU, China, and the U.S. were presented above. These concepts are what encourage these three legal systems to build different regulations to protect the "right to be let alone."[128]

Indeed, the variation in concepts of privacy is what makes legal systems protect privacy through different regulations, which are sometimes sectored, and in others, a potent and unified regulation. Each legal system aggregates the value of privacy in-laws or directives. Indeed, the variation of privacy concepts is what makes legal systems protect privacy through different regulations, sometimes sectored, in others, as a potent and unified regulation. Each legal system aggregates the value of privacy in-laws or directives.

2.6 Data Protection

Data protection is directly linked to privacy because it emerges with the necessity to protect individuals and their information utilized for commercial purposes. It aims to safeguard them from public interference or from having their private information completely disclosed. Nonetheless, protecting personal information in the digital world has increased the need for regulations. Almost all countries have some regulations related to data protection. The variations are that some countries regulate data in strict ways, and other countries regulate data according to relationships

[127] CHRISTOPHER T. ANGLIM ET AL., PRIVACY RIGHTS IN THE DIGITAL AGE, xxi (Grey House Publishing, 2015) (eBook).
[128] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

construed through cultural aspects.[129] The important concept is that data protection regulations exist to preserve peoples' identities and prevent others from misusing their information. The goal of data protection laws is to embrace mechanisms to ensure individuals' privacy because the right to be let alone is not as simple today as in the past. The definition of privacy follows the same concept. However, the methods of providing protection have been evolving with changing technological advancements. In addition, AI tools that involve the constant use of personal data challenge the protection of privacy.

2.6.1 General Data Protection Regulation (GDPR)

Seeking protection of personal data as a fundamental right guarantees the free flow of personal data within the Single Market,[130] and unification of approaches of personal data protection between member states resulted in the adoption of the general data protection regulation by the European Union. After four years of negotiations and reflections, the parliament enacted the General Data Protection Regulation (GDPR)[131] on May 25, 2018. The Information Technology Governance stated,

[129] ALAN CALDER, THE CASE FOR ISO27001:2013, 51 (It government Publishing 2013) (eBook).

[130] Single market, *A single internal market without borders,* European Union, https://europa.eu/european-union/topics/single-market_en (last visited Apr.13.2020).

[131] As known technology has been changed faster, than any regulation cannot manage it. Before, the GDPR, EU adopted the Directive 95/46/EC**,** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Nonetheless, with the advent of new technologies, the commission through a comprehensive protection strategy on data protection in the European Union launched a communication to reflect on the new challenges for the protection of personal data. After conduct studies and investigations, the Commission found that one of the issues were the definition of personal data. The directive was flexible and broad when defining the scope of personal data. For instance, how personal data should be protected in different areas and what is personal data in those areas. Also, the lack of harmonization between the state's members. Some countries would be more or less strict when applying the directive. Thus, some of these facts prompt a deep investigation with the aim to establish a legislative framework that would be valid through the test of time**.**

European Commission Communication from the Commission to the European Parliament, *the Council, the Economic and Social Committee and the Committee of the Regions: a comprehensive approach on personal data protection in*

> The GDPR is the latest step in the ongoing global recognition of the value and importance of personal information. Although the information economy has existed for some time, the real value of personal data has only become more recently evident. Cyber theft of personal data exposes people to significant personal risks. Big data analysis techniques enable organizations to track and predict individual behavior, and can be deployed in automated decision-making.[132]

Thus, all risks to which a person is exposed when using the Internet prompted the EU to create a robust regulation to safeguard the right of privacy, conferred in Article 8 of the European Convention of Human Rights.[133] Besides, the European Charter of Fundamental Rights, Articles 7 and 8[134] explicitly provide for the right to protect personal data. With these concepts, the EU through the GPDR protects any information that can identify an individual, such as their name, date of birth, photographs, email address, the movement of personal data, and fundamental rights.[135]

the European Union, COM (2010) 609 (Nov.04. 2011). This document gives a clue how the EU Commission was working to achieve the robust GDPR. See also, European Data Protection Supervisor, *The History of the General Data Protection Regulation,* https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Apr.12.2020).This webpage gives an overview of the data protection history since the Directive 95/46/EC until the GDPR. See also Viviane Reding, Privacy matters – *Why the EU needs new personal data protection rules*, The European Data Protection and Privacy Conference, Speech /10/70 (Nov.30.2010). In this speech Reding explains the ideas of the data protection reform. Moreover, it introduced the right to be forgotten and why it is time for a reform.

[132] IT Governance Privacy Team, EU GENERAL DATA PROTECTION REGULATION (GDPR), AN IMPLEMENTATION AND COMPLIANCE GUIDE, ch.1 (3th ed., IT Governance Publishing, 2019) (eBook).

[133]Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
European Convention of Human Rights art. 8, 1953, https://www.echr.coe.int/Documents/Convention_ENG.pdf .

[134] Respect for private and family life everyone has the right to respect for his or her private and family life, home and communications. European Convention of Human Rights art. 7, 1953, https://www.echr.coe.int/Documents/Convention_ENG.pdf .

[135] "Article 1 Subject Matter and Objectives
1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."
REGULATION (EU) (GDPR) 2016/679, art. 1, 2016 O.J. (L 119/32).

The European Data Protection Supervisor states

> Fully applicable across the EU in May 2018, the GDPR is the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age. It applies to organizations or companies not established in the EU that offer goods and services to individuals in the EU or monitor their behavior. It creates new rights for individuals in the digital environment and several new and detailed obligations for cooperation.[136]

Therefore, the GDPR gives a concrete answer to the challenges this digital era has brought to all individual consumers, securing them the right to have their privacy safe. It is an important advance in terms of regulations, which also encourages other countries to emulate the EU example. Thus, countries seeking to negotiate with the EU, need to comply with the law. It means that the GDPR benefits all individuals around the world by guiding governments and legislators to reflect and give attention to an essential topic: the dangers that technological advances pose if they are not properly regulated.

Willian RM Long et al. address the scope of EU regulation in these terms: "Although the GDPR sets out harmonized data protection standards and principles, the GDPR grants EU Member States the power to maintain or introduce national provisions to further specify the application of the GDPR in State Law."[137] It creates a consistent security protection system because all states are applying the same law.

To apply these rules, the GDPR relies on Data Protection Authorities (DPAs); and, for "enforcement of data protection laws to be effective, DPAs are given the power to investigate, detect and punish violations as well as the responsibility to raise awareness of data protection rights

[136] European Data Protection Supervisor, The EU'S independent data protection authority, *Data Protection* https://edps.europa.eu/data-protection/data-protection_en (last visited 01/18/2020).
[137] WILLIAN RM ET AL., EU OVERVIEW, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW, 5 (6th ed. 2019).

and obligations in general."[138] These powers are essential in the regulation for guaranteeing its application. DPAs establish a trustful relationship between society and corporations. In addition, to provide confidence, the DPAs cannot be connected with governments or political parties and need to be independent agencies that fulfill a sense of credibility, which means that the execution and application of the regulation are free from direct and indirect influence.

Furthermore, the European data protection supervisor believes the following about privacy, data protection, and security challenges: "The rights to privacy and data protection may need to be balanced against other EU values, human rights, or public and private interests such as the fundamental rights to freedom of expression, freedom of press or freedom of access to information."[139] Therefore, it appears that through threats and internal regulations, the EU is managing data security and data share. The digital era poses challenges to data protection, including the fact that laws take a lot of time to be enforced, and technological advances take nanoseconds to deliver something new. Put differently, laws are often playing catchup with technological advances.

Moreover, the GDPR in Article 4 defines what is considered personal data for the purposes of the regulation:

> (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[140]

[138] European Data Protection Supervisor, The EU'S independent data protection authority, *Data Protection*, https://edps.europa.eu/data-protection/data-protection_en (last visited 01/18/2020).

[139] *Id.*

[140] REGULATION (EU) (GDPR) 2016/679, art. 4, 2016 O.J. (L 119/33).

Regardless of this definition, the key point is that personal data includes every single data that permits the identification of an individual. This definition, provides safety for EU citizens and responsibility for businesses when collecting personal data. Another important point is stated in Article 5,[141] which provides principles relating to the processing of personal data. This regulation through seven principles sets out the requirements when dealing with personal data. Article 5 works as a guide for companies and also gives individuals the power to have their data deleted, corrected, and anonymized. The GDPR gives individuals in the EU the ability to control their personal data.

It would, therefore, appear that the GDPR gives EU individuals the right to access personal data collected to be informed. Companies need to be transparent by showing how data will be used. Individuals have the right to rectification if the data is incomplete or wrong. The GDPR empowers individuals with the right to erase, known as the right to be forgotten. It also guarantees individuals the right to know about data portability relating to automated decision making, giving them the power to object and restrict the processing of personal data. This is particularly useful when they are not sure how the data will be used.[142] Because of all these rights conferred to EU individuals,

[141] Article 5, "1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) 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 in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization'); (d) 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 ('accuracy'); (e) 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 in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."
REGULATION (EU) (GDPR) 2016/679, art. 5, 2016 O.J. (L 119/33).

[142] Article 15, "The right of Access" REGULATION (EU) (GDPR) 2016/679, art. 15, 2016 O.J. (L 119/43).

the GDPR is the strongest data protection law in the world because it returns to people the right to privacy, protecting it as a fundamental right.

2.6.2 China- Cybersecurity Law of the People's Republic of China (CSL)

The Cybersecurity Law (CSL), the principal data protection in China, was enacted on June 1, 2017. Article 2 of the law states, "The law is applicable to the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China."[143] Under this law, every company that uses a computer network to provide services needs to comply with the law. In addition, the state council will set up the specific scope and protection inside the critical areas defined in Article 31.[144] Moreover, China has other laws that have an impact on data protection. Hongquan (Samuel) Yang states the following:

Article 13 and 14 "The right to be informed" REGULATION (EU) (GDPR) 2016/679, art. 13, 2016 O.J. (L 119/40). REGULATION (EU) (GDPR) 2016/679, art. 14, 2016 O.J. (L 119/41).
Article 16 and 19 "The right to rectification" REGULATION (EU) (GDPR) 2016/679, art. 16, 2016 O.J. (L 119/43). REGULATION (EU) (GDPR) 2016/679, art. 19, 2016 O.J. (L 119/45).
Article 17 and 19 "The right to erasure" REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/43).
Article 18 "The right of restriction" REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/44). REGULATION (EU) (GDPR) 2016/679, art. 19, 2016 O.J. (L 119/45).
Article 20 "The right data portability" REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/45).
Article "The rights in relation to automated decision making, including profiling"
REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/46).
Article 21 "The right to object" REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/46).

[143] Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), NEW AMERICA (2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ .

[144] "Article 31: The State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure."
Translation: Cybersecurity Law of the People's Republic of China, *supra* note 143.

> [t]he official implementation of the CSL marks the gradual formation of China's new legal framework for cybersecurity on data protection. Among other things, the CSL covers the following aspects:
> a personal information protection;
> b general network protection obligations of the operators and the multi-level protection scheme (MLPS);
> c enhanced protection for the critical information infrastructure (CII);
> d data localization and security assessment for the cross-border transfer of personal information and important data; and
> e security review of the network products and services.[145]

The CSL seems to cover a variety of important topics related to data protection. However, other laws also implement other regulations and national standards, since the CSL does not provide, in detail, how it works in practice. Chapter 1 of the CLS refers to other laws that regulate data protection and must be followed by network operators, carrying out business and service activities, according to Chapter 1, Article 9 of the provision.

Furthermore, an important detail in the CSL relates to data localization, addressed in Chapter 3 Article 37, which states as follows: "Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China shall store it within mainland China."[146] Thus, the data collected in China cannot be transferred outside the territorial limits of China, unless the state council authorizes it or the law has a provision that allows its transfer. Thus, the government keeps control of the flow of data from foreign collection. However, as will be discussed later, the government of China appears to be more interested in creating a monopoly over data within the territory of China rather than the protection of personal data. Another important point stated in Article 21 is the responsibility of companies to safeguard the personal information collected through the cybersecurity multi-level protection system (MLPS). These measures are to prevent

[145] Hongquan (Samuel) Yang, *China*, in THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 115 (6th ed. 2019).

[146]Translation: Cybersecurity Law of the People's Republic of China, *supra* note 143.

computer viruses, cyberattacks, and encryption by mentioning that companies need to comply with other obligations provided by law. Thus, the CSL is a guide, which in some articles, provides only broad concepts that are clarified in other administrative laws.[147]

In addition, the regulation asserts in Article 41 that "network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall publish rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the persons whose data is gathered."[148] Hence, corporations need to collect data only related to their business purposes and have permission to collect such data from the consumer. In the following Articles 42 and 43, the provision states that personal information must not be disclosed or shared. On the other hand, after processing the information provided, the operator needs to verify there is no way to identify any personal information. It is also clear that, in case of accidents, such as loss or discharge of information, users and government authorities shall be informed. This requirement suggests an atmosphere of credibility between companies, governments, and people. Article 44 also safeguards personal data: "Individuals or organizations must not steal or use other illegal methods to acquire personal information and must not unlawfully sell or unlawfully provide others with personal information."[149]

Another interesting point is that Article 47 states that network operators are responsible for the comments people publish. For instance, if the law prohibits some subjects, the network operator must delete the information and report it to the government department. The prohibition

[147] Translation: Cybersecurity Law of the People's Republic of China, supra note 143, at Article 21.
[148] *Id.* at Article 41
[149] Translation: Cybersecurity Law of the People's Republic of China, *supra* note 143, at Article 47.

of certain types of content seems to be a form of control of people by the government rather than data protection.

Another relevant aspect is that the cybersecurity regulators are responsible for enforcing the law and punishing infractions. As regulators of cybersecurity, China has the Ministry of Public Security (MPS), who is the lead regulator, working with other regulators, including the Cyberspace Administration of China (CAC) and the Ministry of Industry and Information Technology (MIT).[150] Thus, working together, the MPS, CAC, and MIT enforce the law and apply the rules to keep network operators and people inside a vigilant and controlled cyberspace where fines are applied and people posting forbidden subjects are arrested or have their content deleted by the operators.

Furthermore, Article 47[151] states that network operators are required to oversee all information published and if information is forbidden, for example political beliefs opposing the government, the network operator needs to delete the content and report the personal identity to the relevant government authorities. This article overrides the right of anonymity, freedom of speech, and the right to privacy. It seems that when the subject is government surveillance and control of people, the law paces privacy on a second plane.[152]

[150] Yan Luo, Zhijing et al.,*Cyber Trends in China*, *Cyber requirements in China,* LEXOLOGY (2019), https://www.lexology.com/library/detail.aspx?g=2352790f-4414-484d-814e-6c435d3e1956 (last visited Jan 21, 2020).

[151] "Article 47**:** Network operators shall strengthen management of information published by users and, upon discovering information that the law or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ handling measures such as deleting the information, prevent the information from spreading, save relevant records, and report to the relevant competent departments." Translation: Cybersecurity Law of the People's Republic of China, *supra* note 143, at Article 47.

[152] See Ulrike Franke, *Harnessing Artificial Intelligence, European Council on Foreign Relations, 4* (Jul. 2019). "Authoritarian states have advantages over democratic ones when it comes to data. China's relatively weak data privacy protections give data aggregators a freer hand in what they can do with what they collect. And the government can access personal data for reasons of public or national security without the same legal constraints a democracy would face." The author explains that authoritarian government has the alternatives ways to make companies to comply with rules.

It can be concluded that there is no one law that addresses all rules in China about data protection. This makes it a little difficult to interpret different laws that apply to the same subject. Similar to other countries, the Cybersecurity Security Law of China is new and will requires many revisions to properly limit and regulate all technological advances. The positive point is that governments are concerned about personal data and the implications of corporations using data without limitations. Thus, the set of laws that provides privacy protection complement each other but do not provide adequate protection to data. Similar to the GDPR, the CSL is suffering from the need for amendments and also requires guidelines that help companies comply with the law. Notwithstanding the data protection laws, Chinese regulations on data protection and how the governance is structured in China as an authoritarian state has, for many years, deprived people of their fundamental rights. So, the citizens do not have the awareness or expectations of protection that exist in the west.[153] Maybe the Chinese regulations are actually meant to regulate foreign companies in China, controlling the flow of personal data and limiting individuals' liberty, anonymity, and free speech through regulations.[154]

2.6.3 United States: Data Protection Framework

In the United States, there is no unified law that defines data protection. There are a comprehensive number of laws that regulate data protection known in the U.S. as Information Privacy Law. Daniel J. Solove notes that “information privacy law consists of a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges,

[153] Jack Wagner, *China’s Cybersecurity Law: What You Need to Know,* The Diplomat (Jun. 2017).
[154] See Kristin Shi-Kupfer et al., *China’s Digital Rise Challenges for Europe*, 7 Merics Papers on China 23 (Apr.2019).

property law, and contract law."[155] Furthermore, the state statutory law will vary from state to state. The U.S. Constitution and federal law are considered supreme laws that guide the states. In this way, state law cannot be more restrictive than federal law. Before an overview of the United States framework, it is crucial to comprehend that most of the laws are directly connected to judicial decisions, which means the common law system. Allan Charles Raul points out that,

> The United States has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk:
> a financial, insurance and medical information;
> b information about children and students;
> c telephone, Internet and other electronic communications and records;
> d credit and consumer reports and background investigations at the federal level; and
> e a further extensive array of specific privacy laws at the state level.[156]

Because of these specifications, privacy protection is considered sectored.

The privacy protection in tort law through the restatement encompasses four privacy torts. Solove et al. observe the following:

> Public disclosure of private facts. This tort creates a cause of action for one who publicly discloses a private matter that is 'highly offensive to a reasonable person' and 'is not of legitimate concern to the public.
> Intrusion upon Seclusion. This tort provides a remedy when one intrudes 'upon the solicitude or seclusion of another or his private affairs or concerns' if the intrusion is 'highly offensive to a reasonable person.'
> False light. This tort creates a cause of action when one publicly discloses a matter that places a person 'in a false light' that is 'highly offensive to a reasonable person.'
> Appropriation. Under this tort, a plaintiff has a remedy against one 'who appropriates to his own use or benefit the name or likeness' of the plaintiff.[157]

Thus, in the four situations listed above, tort law regulates privacy protection. However, not all states recognize these torts; some apply two or three of these concepts and others all four. Besides

[155] SOLOVE, *supra* note 17, at 56.
[156] ALAN CHARLES RAUL ET AL., UNITED STATES: OVERVIEW, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW, 368 (4th ed. 2017).
[157] SOLOVE ET AL., *supra* note 117, at 30, 31.

this, privacy is protected in evidence law. Solove et al. state that "the law of evidence has recognized the importance of protecting the privacy of communications between attorney and client, priest and penitent, husband and wife, physician and patient, and psychotherapist and patient."[158] Evidence law is an important law because it confers protection for personal information shared in confidentiality that cannot be inquired into legal contexts during a process or trial.

Under some circumstances, the United States may provide property rights in information. These rights suggest that personal data is someone's property and the use of this property without permission is illegal. [159] Contract law also provides privacy protection. According to Solove et al., "Contract often functions as a way of sidestepping state and federal privacy laws. Many employers make employees consent to drug testing as well as e-mail and workplace surveillance in their employment contracts."[160] The use of these contracts to protect information shared inside corporations brings confidentiality inside the workplace and between people who are negotiating through a contract. In the scope of criminal law, privacy is protected. As an example, Solove et al. state, "The crime of blackmail prohibits coercing an individual by threatening to expose her personal secrets. Many of the statutes protecting privacy also contain criminal penalties, such as statutes pertaining to wiretapping and identity theft."[161] Hence, there is also an important approach in criminal law to privacy protection.

Although the United States Constitution does not explicitly use the term privacy, it has some provisions that protect privacy. For instance, the First Amendment safeguards privacy, the Third Amendment protects the privacy of the home, and the Fourth Amendment states that people

[158] SOLOVE, *supra* note 17, at 31.
[159] Id. at 32.
[160] *Id.* at 32.
[161] SOLOVE ET AL., *supra* note 117, at 32.

have the right to be secure in their houses.[162] However, this is not a unified concept in all states' constitutions. Moreover, federal acts, statutory laws, and state regulations, covering many sectors, have a comprehensive number of statutory laws that protect privacy in technology, health, business, and so on. Alan Charles Raul et al. assert, "Federal and state authorities, as well as private parties through litigation, actively enforce these laws, and companies also, in the shadow of this enforcement, take steps to regulate themselves."[163] Nonetheless, if federal law does not cover the variety of subjects that privacy includes, then the Federal Trade Commission (FTC)[164] Act will fill gaps enforcing laws that protect consumers.

As it is apparent from the discussion above, the U.S. has several laws to regulate data protection. The Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.)[165] (DDPA) regulates drivers' personal information. The U.S. also has privacy laws that impact specific sectors. For example, the Gramm Leach Bliley Act (GBLA) (15 U.S.C. § 6802 (a) et seq.), "requires financial institutions-companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard sensitive data."[166] The GBLA is a crucial privacy law in transactions involving financial institutions. Another significant law is the Health Information Portability and Accountability Act, as amended (HIPAA) (29 U.S.C § 1181 et seq.), which provides

[162] *Id.* at 33.

[163] ALAN CHARLES RAUL ET AL., *supra* note 156, at 401.

[164] "The Federal Trade Commission Act is the primary statute of the Commission. Under this Act, as amended, the Commission is empowered, among other things, to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress and the public. A number of other statutes listed here are enforced under the FTC Act." Federal Trade Commission Act, *FEDERAL TRADE COMMISSION* (2018), https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act (last visited Jan 23, 2020).

[165] 18 U.S.C. § 2721 (1994).

[166] Federal Trade Commission Protecting American's Consumers, *Gramm-Leach-Bliley Act*, https://bit.ly/2IlysBF (last visited Jan 23, 2020).

confidentiality for all personal information related to healthcare and establishes restrictions on the disclosure of personal data.[167]

Another important regulation is "The Cybersecurity Act, passed in 2015 which includes a Cybersecurity Information Sharing Act (CISA). CISA is designed to foster cyberthreat information sharing and to provide certain liability shields related to such sharing and other cyber-preparedness."[168] Thus, a set of laws provides vast protection for privacy in different sectors. Other important laws addressed by Willian Stallings include the following:

> The Family Educational Rights and Privacy Act of 1974 (FERPA): Protects students and their families by ensuring the privacy of student educational records.
> The Fair and Accurate Credit Transaction Act of 2003 (FACTA): Requires entities engaged in certain kinds of consumer financial transactions (predominantly credit transactions) to be aware of the warning signs of identifying theft and to take steps to respond to suspected incidents of identity theft.
> Federal Policy for the Protection of Human Subjects: Published in 1991 and codified in separate regulations by 15 federal departments and agencies, outlines the basic ethical principles (including privacy and confidentiality) in research involving human subjects.
> The Children's Online Privacy Protection Act (COPPA): Governs the online collection of personal information from children under the age of 13.
> The Electronic Communications Privacy Act: Generally, prohibits unauthorized and intentional interception of wire and electronic communications during the transmission phase and unauthorized accessing of electronically stored wire and electronic communications.[169]

The set of comprehensive laws in the United States was created to cover some sectors, which makes them specific. In other words, these laws were enacted to regulate transactions in a certain field, and protect and forbid some acts. On the other hand, Preston Bukaty asserts

> The lack of comprehensive privacy regulation in the US presents a unique set of compliance challenges for companies that collect personal data. Although a

[167] Center for Disease Control and Prevention, *Health Insurance Portability and Accountability Act of 1996 (HIPAA*), https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited Jan 24, 2020.

[168] ALAN CHARLES RAUL ET AL., *supra* note 156, at 371.

[169] WILLIAN STARLING, INFORMATION PRIVACY ENGINEERING AND PRIVACY BY DESIGN: UNDERSTANDING PRIVACY THREATS, TECHNOLOGY, AND REGULATIONS BASED ON STANDARDS AND BEST PRACTICES ch.3 (Addison-Wesley Professional, 2019).

> patchwork of sector-specific and state laws exist, they rarely deal with the pervasive collection and sale of people's personal information. Penalties for data breaches attempt to protect personal information by punishing companies for after-the-fact violations, but this does little to safeguard information in real time.[170]

The fact that the country has a comprehensive set of laws does not mean it caters to personal data and treats everything as personal data. Legislators and courts are still dealing with the lack of a strong law. According to Alan Charles Raul,

> To address concerns about privacy practices in various industries, industry stakeholders have worked with the government, academics and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively developed accountability programmes establish expected practices for use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities.[171]

This is what makes private information protection complicated, and sometimes places decisions in the hands of private companies. The following table includes a list of important federal laws that relate to privacy[172]

[170] PRESTON BUKATY, CALIFORNIA CONSUMER PRIVACY ACT (CCPA): AN IMPLEMENTATION GUIDE (2019) (eBook).
[171] ALAN CHARLES RAUL ET AL., *supra* note 156, at 372.
[172] STARLING, *supra* note 169, at ch.3.

Table 1.
List of Federal laws related to privacy.

Category	Federal Law	Date
Health Care	Health Insurance Portability and Accountability Act (HIPAA)	1996
	Health Information Technology for Economic and Clinical Health (HITECH) Act	2009
Genetics research	DNA identification Act	1994
	Genetic Information Nondiscrimination Act (GINA)	2008
Business/ workplace	Children's Online Privacy Protection Act (COPA)	1998
	Controlling the assault of Non-solicited Pornography and Marketing (CAN-SPAM) Act	2003
Financial sector	Gramm-Leach- Bliley Act (GLBA)	1990
	Fair Credit Reporting Act (FCRA)	1970
	Fair and Accurate Credit Transactions Act	2003
	Right to Financial Privacy Act	1978
Educational/ students	Family Educational Rights and Privacy Act (FERPA)	1974
Law enforcement	Omnibus Crime Control and Safe Streets Act	1968
	Electronic Communications Privacy Act (ECPA)	1986
National security	The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act)	2001
	Real ID Act	2005
Government	Freedom of Information Act (FOIA)	1966
	The Drivers Privacy Protection Act	1994
	Privacy Act of 1974	1974
	Computer Matching and Privacy Protection Act	1988
	E-Government Act	2002
	Federal Information Security Management Act (FISMA)	2002

Nonetheless, one state has been at the top of the list concerning a complete regulation of privacy. Through the California Consumer Privacy Act (CCPA), California is leading the United States with a strong policy in privacy protection. The CCPA comes from the necessity to preserve personal information after the scandal involving the National Security Agency (NSA) and large companies, such as Google, Facebook, Yahoo, and Microsoft, which are located in Silicon Valley. Californians for Consumer Privacy is an organization focused on protecting and expanding privacy rights for consumers, which sponsors the CCPA. The new regulation accomplishes the following goals:

> You will have the right to know what information large corporations are collecting about you…and you should. Businesses use your personal information for their own purposes, including targeting you with ads, discriminating against you based on price or service level, and compiling your information into an extensive electronic file on you. You should be able to know what is being collected about you. You will have the right to tell a business not to share or sell your personal information...and you should. California law has not kept pace with changing business practices. Businesses not only know where you live and how many children you have but also how fast you drive, your personality, sleep habits, health, and financial information, current location, web browsing history, to name just a few things.
> You will have the right to protections against businesses which do not uphold the value of your privacy...and you should. Businesses that collect your sensitive personal information should take basic steps to keep it safe. Right now there are no consequences if they don't, and this law will introduce some consequences.[173]

It therefore appears that the CCPA is a concrete answer for the indiscriminate amount of personal data that businesses have commercialized or shared without authorization, generating millions of dollars. The CCPA gives back to consumers the right to control their personal information, which is an accomplishment in the technological age. The CCPA is being compared with the European Union General Data Protection Regulation (GDPR), although it should be noted that the CCPA has more prescriptive requirements than the GDPR. Thus, the CCPA protects consumers who live in California and covers businesses in California that collect the personal information of California residents and have gross revenues exceeding $25 million (adjusted by inflation); sell or share

[173] Californians for Consumer Privacy, *About the Initiative: California Consumer Privacy Act*, *About the Initiative California Consumer Privacy Ac: What goals does the California Consumer Privacy Act accomplish?* https://www.caprivacy.org/about , (last visited Jan 25, 2020).

information of 50,000 or more consumers, householders, or devices; and, derive 50 percent or more of their annual revenues from selling consumers' personal information.[174] Another interesting aspect of the CCPA is that the law empowers consumers with the right to request the deletion of any personal information.[175] Besides this, the law also requires businesses to inform consumers, either before or in the moment of collection of personal information, of their purposes. When not informed, consumers have the right to request this information. Effective January 1, 2020, the CCPA section 1798.140(c) (1), defines the type of business to which it applies as follows:

> A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information that does business in the State of California.[176]

Therefore, the CCPA applies to a business that processes personal information and is located in the state of California. Section 1798.140(c) (2), also addresses the following:

> Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. 'Control' or 'controlled' means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. 'Common branding' means a shared name, service mark, or trademark.[177]

In this way, subsidiaries also need to comply with the regulation according to the control exercised. Among important definitions, the CCPA defines personal information, which is the scope of the

[174]CAL. CIV. CODE §1798.140(a) (b) (1).

[175] CAL. CIV. CODE § 1798.105(a) (West 2018).

[176] CAL. CIV. CODE § 1798.140(c) (1) (West 2018).

[177] CAL. CIV. CODE § 1798.140(c) (2) (West 2018).

regulation. Section 1798.140 (o) (1) states that "personal information" means "information that identifies, relates to, describes, if it is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[178] Accordingly, with this definition and an exemplified non-exhaustive list, the CCPA states the coverage of personal information, which limits corporations' abilities to exploit personal information without boundaries. Notwithstanding, the CCPA does more than provide protection; it supports individuals' understanding of how data is collected, disclosed, and sold. It gives security, trust, and transparency to the relationship between consumers and enterprises. The CCPA gives to individuals the power to share personal information or not, according to their expectations and beliefs.

As expressed above, the CCPA is a new law that was enacted in January of 2020. However, the rulemaking process is still developing until the enforcement of the law on July 1, 2020. Since January, companies have criticized the CCPA for a lack of clarity in some parts of the law as well as the difficulty of interpreting the rules.[179] Because of this, in the implementation phase on February 10, 2020, the California Attorney General (AG) Xavier Becerra released modifications to the proposed regulations relating to the CCPA. The objective was to receive comments about the law. The document also was an opening dialogue between companies, experts, attorneys, and everyone else who will need to comply with the CCPA when dealing with personal data. Those

[178] CAL. CIV. CODE § 1798.140(o) (1) (West 2018).

[179] See Angelique Carson, *Critics say attorney general's proposed CCPA regulations add confusion, not clarity*, iapp, https://iapp.org/news/a/critics-say-ags-proposed-ccpa-regulations-add-confusion-not-clarity/
(last visited Apr.14.2020). See also, Sara Morrison, *California's new privacy law, explained, The California Consumer Privacy Act gives Californians some control over their data, but only if they know how to take advantage of it* Vox, (Dec.30,2019),
https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained

who are affected by the law or have concerns are seeking further clarification.[180] The hearings produced a document of 784 pages with several different comments. After answering each one of these comments, the AG updated a new draft. The most relevant points are in Section 179840(o) (1),[181] which give guidance on the interpretation of personal information. This section also increases the number of exceptions regarding when a service provider can use personal data. Civil Code Section 1798.99.80, according to the draft, allows a business "that does not collect personal information directly to a consumer and is registered with the AG as a data broker does not need to provide a notice at the collection to the consumer"[182]

In the section on Notice of Financial Incentive, the draft provides clarification in nondiscriminatory and discriminatory practices. It explains these practices through an example of what financial incentives and discriminatory practices are. The draft also provides detailed information about the general principles a company's privacy policy shall include. In the section on the notice for the collection of personal data, examples are provided on how a business will comply with the regulation when collecting personal data from a mobile device.[183]

[180] Xavier Becerra, Attorney General, *California Consumer Privacy Act (CCPA), Modifications to proposed Regulations – released February 10, 2020 15 day Comment Period- ended February 25, 2020*. (Feb.10.2020) https://oag.ca.gov/privacy/ccpa. All documents hearing can be accessed through the website
See Heather Egan Sussman et al, *California Attorney General Releases Updated Drafts of Proposed CCPA Regulations*, Orrick Blog (Feb.13,2020), https://blogs.orrick.com/trustanchor/2020/02/13/california-attorney-general-releases-updated-drafts-of-proposed-ccpa-regulations/

[181] Section 179840(o) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:" CAL. CIV. CODE § 1798.140(o) (1) (West 2018).

[182] Xavier Becerra, Attorney General, California Consumer Privacy Act (CCPA), Text of Regulations (Clean Version) -15 Day Comment Period- February 7- 24,2020, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf? See also the original before the draft. CAL. CIV. CODE § 1798.99.80. (d) (West 2018).

[183] Heather Egan Sussman et al, *California Attorney General Releases Updated Drafts of Proposed CCPA Regulations*, *Orrick* Blog (Feb.13,2020), https://blogs.orrick.com/trustanchor/2020/02/13/california-attorney-general-releases-updated-drafts-of-proposed-ccpa-regulations/

On March 11, 2020, the AG launched the second set of modifications similar to those issued in February with a deadline to submit written comments on March 27, 2020.[184] The second written comments document had 484 pages, and again, the AG will respond to each one of the comments. The second set of modifications did not expand the subject matter in the CCPA. It merely brought adjustments in the same topics of the released February draft. For instance, included in the definitions are employment benefits and employment-related information. The term "financial incentive" changed the designation "as compensation for disclosure, deletion" to "related to collection, retention" which clarifies for business what is a financial incentive and when it applies. The guidance regarding the interpretation of CCPA was completely deleted. It also brings an overview of required notices requiring that businesses operating in selling personal information "shall provide a notice of right to opt-out."[185] Following other alterations, in the notice at the collection of personal data, it offers more details about reasonable access to consumers with a disability and businesses collecting information through a mobile application. An important alteration in this section is that the business that does not collect personal information from consumers does not need to provide notice. Also, businesses collecting employment personal information do not need to provide a link saying "do not sell my information."[186] The privacy

[184] Xavier Becerra, Attorney General, California Consumer Privacy Act (CCPA), *Modifications to proposed Regulations – released March 11, 2020 Deadline to Submit written Comments: March 27, 2020 at 5 pm* (March 11.2020) https://oag.ca.gov/privacy/ccpa .

[185] Xavier Becerra, Attorney General, *California Consumer Privacy Act (CCPA), 2nd Set of Modifications to Proposed Regulations* **-** *released March 11, 2020 Deadline to Submit Written Comments: March 27, 2020 at 5 p.m.*, State of California Department of Justice (Mar.11,2020), *https://oag.ca.gov/privacy/ccpa* See the text with all modifications here Text of Second Set of Modified Regulations – Comparison Version, pdf
https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-mod-031120.pdf?
See also Cathy Cosgrove, *Analyzing the second set of modifications to draft CCPA regulations*, iapp (Mar.17.2020), https://iapp.org/news/a/analyzing-the-second-set-of-modifications-to-draft-ccpa-regulations/

[186] Xavier Becerra, Attorney General, *California Consumer Privacy Act (CCPA), 2nd Set of Modifications to Proposed Regulations* **-** *released March 11, 2020 Deadline to Submit Written Comments: March 27, 2020 at 5 p.m.*, State of California Department of Justice (Mar.11,2020), *https://oag.ca.gov/privacy/ccpa* See the text with all modifications here Text of Second Set of Modified Regulations – Comparison Version, pdf

policy section includes a statement that companies need to identify the categories of sources from which the personal information is collected and also need to create ways for consumers to understand the companies' purposes for collecting personal data. This means they must explain to consumers what the personal data is used for. In the section responding to requests to know and requests to delete, a business is forbidden to disclose sensitive data such as social security numbers, driver licensees, or other documents. However, the business shall inform the consumer when collecting this type of data. Another important modification in this section deals with situations when a business denies a consumer's request to delete personal information. It is the business's obligation to ask if the consumer would like to opt-out of the sale of their data. Also, clarification in this second draft allows service providers to collect information about consumers when assisting other businesses.[187] These initiatives show that California, in order to have a strong rule on protection of personal data, is seeking to have an effective regulation. The hearings and written opinions are designed to help fill gaps and clarify the law, making it easier for companies to comply and for consumers to understand that privacy matters. The CCPA has been copied by many states. According to Mitchell Noordyke, "Although many of the bills included in the table will fail to become law, comparing the key provisions in each bill can help understand how privacy is developing in the United States."[188] To better understand how large the privacy universe is in the United States, and how the CCPA has influenced other states to write privacy bills, Table 2 provides an illustrative table of comprehensive privacy law comparisons.[189]

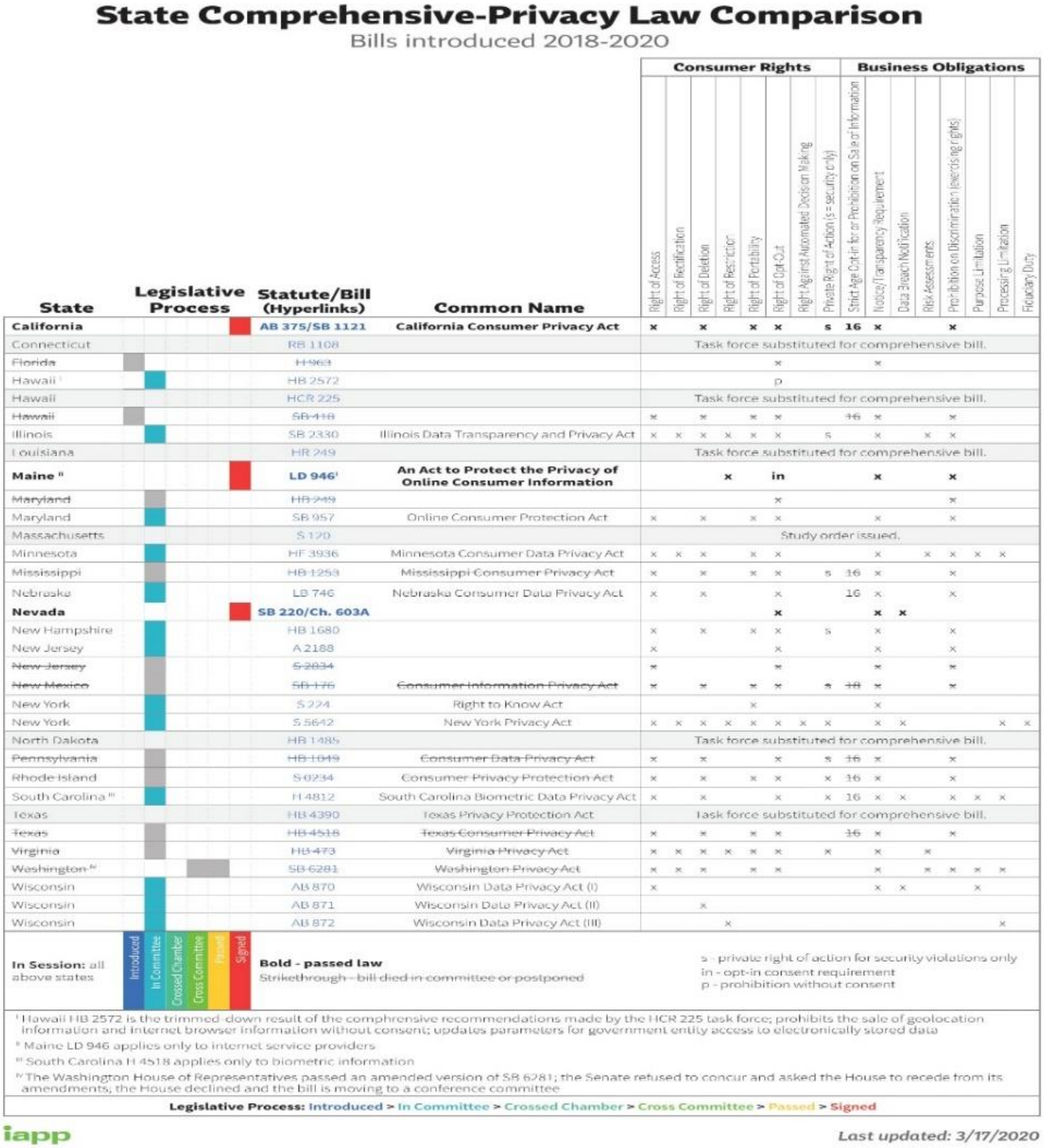
[187] Becerra, *supra* note 185.

[188] Mitchell Noordyke, *US state comprehensive privacy law comparison US state comprehensive privacy law comparison*, IAPP (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison

[189] *Id.*

Table 2

Table of Privacy Law Bills



State Comprehensive-Privacy Law Comparison

Bills introduced 2018-2020

State	Legislative Process						Statute/Bill (Hyperlinks)	Common Name	Consumer Rights								Business Obligations							
									Right of Access	Right of Rectification	Right of Deletion	Right of Restriction	Right of Portability	Right of Opt-Out	Right Against Automated Decision Making	Private Right of Action (s = security only)	Strict Age Opt-In for or Prohibition on Sale of Information	Notice/Transparency Requirement	Data Breach Notification	Risk Assessments	Prohibition on Discrimination (exercising rights)	Purpose Limitation	Processing Limitation	Fiduciary Duty
California						■	**AB 375/SB 1121**	**California Consumer Privacy Act**	**x**		**x**		**x**	**x**		**s**	**16**	**x**			**x**			
Connecticut							RB 1108		Task force substituted for comprehensive bill.															
~~Florida~~	▨						~~H 963~~							x				x						
Hawaii [I]		■					HB 2572							p										
Hawaii							HCR 225		Task force substituted for comprehensive bill.															
~~Hawaii~~	▨						~~SB 418~~		x		x		x	x			~~16~~	x			x			
Illinois		■					SB 2330	Illinois Data Transparency and Privacy Act	x	x	x	x	x	x		s		x		x	x			
Louisiana							HR 249		Task force substituted for comprehensive bill.															
Maine [II]						■	**LD 946'**	**An Act to Protect the Privacy of Online Consumer Information**				**x**		**in**				**x**			**x**			
~~Maryland~~		▨					~~HB 249~~							x							x			
Maryland		■					SB 957	Online Consumer Protection Act	x		x		x	x				x			x			
Massachusetts							S 120		Study order issued.															
Minnesota		■					HF 3936	Minnesota Consumer Data Privacy Act	x	x	x		x	x				x		x	x	x	x	
~~Mississippi~~		▨					~~HB 1253~~	~~Mississippi Consumer Privacy Act~~	x		x		x	x		s	~~16~~	x			x			
Nebraska		■					LB 746	Nebraska Consumer Data Privacy Act	x		x			x			16	x			x			
Nevada						■	**SB 220/Ch. 603A**							**x**				**x**	**x**					
New Hampshire		■					HB 1680		x		x		x	x		s		x			x			
New Jersey		■					A 2188		x					x				x			x			
~~New Jersey~~		▨					~~S 2834~~		x					x				x			x			
~~New Mexico~~		▨					~~SB 176~~	~~Consumer Information Privacy Act~~	x		x		x	x		s	~~18~~	x			x			
New York		■					S 224	Right to Know Act					x					x						
New York		■					S 5642	New York Privacy Act	x	x	x	x	x	x	x	x		x	x				x	x
North Dakota							HB 1485		Task force substituted for comprehensive bill.															
~~Pennsylvania~~		▨					~~HB 1049~~	~~Consumer Data Privacy Act~~	x		x			x		s	~~16~~	x			x			
~~Rhode Island~~		▨					~~S 0234~~	~~Consumer Privacy Protection Act~~	x		x		x	x		x	~~16~~	x			x			
South Carolina [III]		■					H 4812	South Carolina Biometric Data Privacy Act	x		x			x		x	16	x	x		x	x	x	
Texas							HB 4390	Texas Privacy Protection Act	Task force substituted for comprehensive bill.															
~~Texas~~		▨					~~HB 4518~~	~~Texas Consumer Privacy Act~~	x		x		x	x			~~16~~	x			x			
~~Virginia~~		▨					~~HB 473~~	~~Virginia Privacy Act~~	x	x	x	x	x	x		x		x		x				
~~Washington [IV]~~				▨	▨		~~SB 6281~~	~~Washington Privacy Act~~	x	x	x		x	x				x		x	x	x	x	
Wisconsin		■					AB 870	Wisconsin Data Privacy Act (I)	x									x	x			x		
Wisconsin		■					AB 871	Wisconsin Data Privacy Act (II)			x													
Wisconsin		■					AB 872	Wisconsin Data Privacy Act (III)				x											x	

In Session: all above states

Introduced | In Committee | Crossed Chamber | Cross Committee | Passed | Signed

Bold - passed law

~~Strikethrough - bill died in committee or postponed~~

s - private right of action for security violations only
in - opt-in consent requirement
p - prohibition without consent

[I] Hawaii HB 2572 is the trimmed-down result of the comphrensive recommendations made by the HCR 225 task force; prohibits the sale of geolocation information and internet browser information without consent; updates parameters for government entity access to electronically stored data

[II] Maine LD 946 applies only to internet service providers

[III] South Carolina H 4518 applies only to biometric information

[IV] The Washington House of Representatives passed an amended version of SB 6281; the Senate refused to concur and asked the House to recede from its amendments; the House declined and the bill is moving to a conference committee

Legislative Process: Introduced > In Committee > Crossed Chamber > Cross Committee > Passed > Signed

iapp

Last updated: 3/17/2020

2.7 The Comparative Approach Between Regulation of AI and Data Protection in the Three Legal Systems

The GDPR clearly states a set of limitations for AI developers, limiting the collection and use of data, automated decision-making, and compliance risks.[190] Under the GDPR, the EU is in an advanced position because it has complete legislation that unifies the requirements in all member states. The data protection also regulates AI under the perspective of human rights, which means protection for citizens is the most important area.

Nonetheless, China provides data protection through the CSL, which has been very strict in punishments. Kai-Fu Lee argued that "China is surpassing leading powers, including the US, in AI and the problems, Facebook faces with regard to data privacy, will not happen in China."[191] According to this expert, China has advantages in data protection because the transfer of data is illegal and is severely punished. However, this punishment does not happen in the same way under the GDPR.

On the other hand, although the United States has a set of data protection laws, there is no exclusive framework for AI. As demonstrated, the framework regulating data protection is sectoral, which means that data are protected in business, medical research, trade secrets, and so on. With the increasing problems and advances around AI, the National Security Commission on AI was created. On August 13, 2018, the John S. McCain National Defense Authorization Act (P.L. 115-232) established the National Security Commission on Artificial Intelligence as an independent Commission "to consider the methods and means necessary to advance the

[190] Daniel Castro and Eline Chivot, *Want Europe to have the best AI? Reform the GDPR*, iapp (Mar, 23.2020), https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/

[191] Cheng Yu, *China ahead of US, EU in AI and Data privacy, experts says*, ChinaDaily.com (Mar. 26.2020), http://www.chinadaily.com.cn/a/201903/26/WS5c99b620a3104842260b29b8.html

development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States."[192] The creation of the National Security Commission on Artificial Intelligence shows the government's concerns. Following this commission, leading attempts have been made to draft a framework for advancing AI while preventing problems with the use of personal data. In January 2020, a memorandum draft for the heads of executive departments and agencies provided guidance for the regulation of AI applications.[193] Thus, some regulations in the AI field will arrive in the near future. The memorandum draft clearly demonstrates that the country will try to balance AI advances and the protection of data.

2.8 General Legal Principles and Requirements for Effective Protection of Data Applied to AI

Privacy and general data protection laws are not specifically aimed at the AI environment. It is obvious from the discussion above that privacy and data protection laws are confronted by a complex technological environment. This environment has been even more complex with the arrival of artificial intelligence.[194] The question of interest is the impact of AI on the protection of privacy and personal data. This is an important question given the nature and function of AI. In the section below, the impact of AI on privacy and data protection will be explored.

AI is a machine that learns from data and provides different examples from the same source. This makes the machine acquire the necessary knowledge to execute tasks effectively and

[192] The National Security Commission, *About,* https://www.nscai.gov/about (last visited Feb.12.2020).

[193] Federal Register the Daily Journal of United States Government, *Request for Comments on a Draft Memorandum to the Heads of Executive Departments and Agencies, "Guidance for Regulation of Artificial Intelligence Applications",* Management and Budget Office (Jan. 13.2020), https://bit.ly/2TqT0z1

[194] J. Van den Hoven et al., *Privacy and information Technology*, Metaphysics Research Lab, Stanford University (Winter, 2019). The authors discuss how technology challenges privacy and the values of privacy.

faster than humans.[195] The increasing use of AI in technology has made AI part of human life. The question is how to control the use of personal data per machine. Since data is everywhere, AI innovations have been using personal data to train programs on how to execute different tasks better and faster than humans. These powerful tools can be found in different places and different forms. Some efforts have been made to create ways to protect society from future problems. With the indiscriminate use of personal data, some authors such as Roger Taylor et al. argue,

> [T]he dangers increase hugely as we adopt computerized decision-making systems driven by big data and machine learning. The scale of the data now available to us means that there is no realistic means to understand the information in our hands without using these technologies. Without transparency, we have no way to know if they are proving beneficial or harmful.[196]

The authors defend the need for transparency by arguing if transparency is not scrutinized, it will not be possible to paint a big picture to recognize whether AI has been used for beneficial achievements or not. Transparency means that companies should be clear about the ways personal data is managed, and they must require authorization before data can be properly used.[197]

The progression of technology and the ways personal information is gathered and processed in companies and governments has transformed the relationship between organizations and individuals.

Taylor et al. affirms,

> Data is no longer a useful tool for implementing decisions; data is increasingly driving decisions, with a rapid feedback loop between what the data tells an organisation about us and the way that the organization then chooses to process the data in future. Power over information today consists more in the control of big data assets than in the ability to conceal specific documents or pieces of information. By that measure, the world is becoming less, not more transparent.[198]

[195] Theodora (Theo) Lau, *When AI Becomes a Part of Our Daily Lives*, Harvard Business Review (May, 23.2019), https://hbr.org/2019/05/when-ai-becomes-a-part-of-our-daily-lives

[196] ROGER TAYLOR AND TIM KELSEY, TRANSPARENCY AND THE OPEN SOCIETY – PRACTICAL LESSONS FOR EFFECTIVE POLICY, 3 (Bristol University Press, 2016).

[197] *Id.*

[198] TAYLOR AND KELSEY, *supra* note 196, at 115.

The amount of data utilized, how the algorithm process is directed, and how the answers about a person are made, does not seem to be clear. These data were collected when an individual executed a specific task, such as posting something on Facebook or answering a health care questionnaire. The question is whether the operators of this data use the data with the utmost human interest.

In the process of building a trustful relationship between society, companies, and government, transparency is an important remaining inquiry. The process needs to be clear, not just in the sense of the right to access information, but also how decisions are made and how the data are managed. Besides, machines have been observing everything humans do. Each click is registered, all to understand consumers' preferences and achieve straightforward purposes in improving sales. However, this collected information can be used for good or bad purposes, and there is no direct warranty. In short, the exchange of free information collected and used by companies and governments that provide human services and commodities, needs to be trustful in a way that everyone can understand the circulation of free information.[199] It is crucial to understand the process of how personal information is used to decide how to approach the subject in a correct way to draft effective laws. The transparency can, in part, satisfy the right to be left alone. This means that a person can decide if he/she wants or does not want to participate in a project by allowing the use of their data. In this way, the power to decide returns to the individual. The innumerable benefits AI provides, such as purchasing items in less time, checking bank balances, and consulting the refrigerator for groceries, also comes with innumerable issues. For instance, there are misappropriations of personal information, data breaches, and consequences of these acts. These acts can be treated with transparency as a key principle related to privacy, since more personal data is being gathered than ever before and this data helps AI become more precise.[200]

[199] *Id*. at116.

[200] Insights Team, *Rethink Privacy For the AI Era*, Forbes (Mar.27.2019),

In spite of this, the Information Commissioner's Office (ICO)[201] published the most evident trade-offs, including the following: privacy versus accuracy and indicating an increasing need for additional personal data to make machine learning more accurate. It is argued that accuracy can have an impact on privacy. The second trade-off is accuracy and fairness, which addresses the issue of AI systems that can lead to biased or discriminatory outcomes. Companies can use techniques to reduce these risks. However, these techniques can reduce accuracy. The third is privacy and fairness, asserting that they might clash in two ways. First, the system can be found inaccurate because of a lack of data information from minority populations. In this case, the corporation needs to collect more personal information in order to become accurate. Second, testing AI fairness will require more personal information that is labeled, because it contains characteristics to test where the system has been fair or not. However, a privacy problem in using this type of data will arise. The third is explainability and accuracy, arguing that simple AI systems are easy to follow and understand how the system operates. Nevertheless, when complex systems, such as machine learning, are hard to follow, including the logic of how the system works, there is a trade-off with explainability. It is an accurate explanation that one system can expose personal information or a company's trade secret.[202] The trade-off analyses are not conclusive, but at least direct attention to important points, which consider open dialogue and reflections between governments, corporations, and society.

https://www.forbes.com/sites/insights-intelai/2019/03/27/rethinking-privacy-for-the-ai-era/#5939ae907f0a

[201] The Information Commissioner's Office (ICO*) is the UK's independent body set up to uphold information rights.* For more information see https://ico.org.uk/about-the-ico/who-we-are/ (last visited Feb.20.2020).

[202] Reuben Binns et al., Information Commissioner's Office, iCO., *Trade-offs*, WIREDGOV (Jul. 25.2019) https://www.wired-gov.net/wg/news.nsf/articles/Tradeoffs+25072019151000?open

2.9 Rethinking Privacy for the AI Era

In the AI era, thinking about privacy seems hopeless. It is necessary to create new boundaries that support technological advances. At the same time, these boundaries must safeguard humanity in conjunction with moral values and privacy, which will have real benefits for society. It is undeniable that AI is fundamental to improve many areas, such as medical research, environment changes, and useful tools that make people's lives easier. However, a balance between human beings and technology is essential. Governments and private companies have started to draw some regulations, and Mercedes Bunz et al. affirm the following:

> Through the development of new assisting technology that can offer new skills and even make decisions, society is for some becoming more inclusive, for others more convenient. On the other hand, questions of algorithmic bias and media recognition arise which concern the issue of whose reality is being technically assisted and who is left out or even who is being discriminated against by automated decisions. For businesses, the liability for the application of this technology making a wrong or biased decision – is currently a difficult grey area.[203]

Thus, it is extremely important to create a framework that protects society from the danger of discrimination, wrong decisions, and privacy invasions. It is important to rethink new regulations for the AI era. An example that illustrates how some private companies have been developing regulations is Intel's AI Privacy Policy White Paper. Through this document, Intel explains how privacy has been protected and assures consumers that their personal data will not be used to harm people. The use of strong encryption and de-identification helps address privacy. However, the company defends the use of data flows and argues that governments should provide open government data to increase AI development through reliable data. [204]

[203] MERCEDES BUNZ AND LAIMA JANCIUTE, ARTIFICIAL INTELLIGENCE AND THE INTERNET OF THINGS UK POLICY OPPORTUNITIES AND CHALLENGES, 13 (CAMRI, 2018).
[204] DAVID HOFFMAN AND RICARDO MASUCCI, INTEL'S AI PRIVACY POLICY WHITE PAPER PROTECTING INDIVIDUALS 'PRIVACY AND DATA IN THE ARTIFICIAL INTELLIGENCE WORLD (Oct. 22, 2018).

Perhaps the key point between governments and corporations is to assure that the advantages AI brings to society are immense and every single effort should be made to enact laws and regulations to keep humans safe. It is also clear that AI will affect society in the economic sector.[205]

[205] See Marcin Szczepański et al, *Economic impacts of artificial intelligence (AI)*, European Parliament (Jul.2019), https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf
In this document the group of researchers stated that there is no consensus on whether AI risks will extend and materialize more. However, with effective policies that would be able to foster the development of AI while checking the negative effects. The briefing presents the economic potential of AI in different regions of the world such as North America, Northern Europe, Latin America, Southern Europe, and others. It also presents the impact on manufacturing, and its effects on firms, industries, and countries. The briefing also points to AI impacts on labor markets and the redistributive effects of AI. See also Evan Sparks, *AI Leadership and the Positive Impacts on Economy, Privacy, Environmental Health*, Forbes (Nov.24.2019), https://bit.ly/2UZxiD3

CHAPTER 3: HOW GLOBAL COMPANIES ARE DEALING WITH DATA PROTECTION AND ARTIFICIAL INTELLIGENCE POTENTIAL RISK

AI is everywhere, and almost all technologies involve some type of AI. Therefore, this chapter focuses on multinational companies and how they are unequivocally facing a real impact in compliance with data protection regulation requirements.

The GDPR and CSL apply to domestic and foreign multinationals. Given the nature of the technology multinational enterprises MNEs,[206] most with any global reach are likely obligated to comply with these regulations, reporting breaches or cyberattacks within 72 hours. They may create a robust protection system to prevent a breach. In the U.S., the CCPA also affects most of the multinational technology companies since most of these corporations are located in Silicon Valley. The law requires that companies inform how personal data is used, with whom this data is shared, and that the companies use strong protection to prevent cyberattacks.[207] According to Frontero, "Today's multinational corporations are faced with the significant challenge of crafting practical procedures to both comply with U.S. obligations *and* meet international privacy standards."[208] Notwithstanding, for multinationals to achieve their AI goals and comply with data protection laws between countries with different standards of privacy protection, they will need to create internal policies to adhere to the most restrictive regulations that will allow them to comply

[206] According to Kojo Yelpaala:" MNE is nevertheless, best understood as an international system that often owns or commands globally significant amounts of technological, financial, managerial, human, or marketing resources." PROFESSOR KOJO YELPAALA, INTERNATIONAL BUSINESS TRANSACTIONS, MCGEORGE SCHOOL OF LAW, 3 (Fall, 2018).

[207] Iapp, *Download "Top 5 Operations Impacts of the California Consumer Privacy Act"(CCPA),* https://iapp.org/l/ccpagd/?gclid=EAIaIQobChMI38jO-sLo5wIVFP5kCh1JSQcnEAAYAiAAEgKVU_D_BwE (last visited Feb.23.2020).

[208] Frontero, *Corporate Counsel's New Big Risk Factor: International Privacy Law and Compliance with U.S. Discovery and Investigation Requests*, Frontero Resources Blog (July, 30, 2018), https://bit.ly/2TIljbm

with the rest of the laws. That is the way to "build trust with consumers and users and stand out from their competitors."[209]

To provide an overview of how corporations manage the implementation of privacy law requirements, the following section comes from International Business Machines Corporation (IBM)'s white paper, "Data Privacy Is the New Strategic Priority."[210] The conclusion of this document illustrates the company's actions:

> Few have full confidence in their ongoing ability to comply with emerging privacy regulations. Those who do often use more mature approaches to policies and standards as well as technology and automation to maintain and scale their strategies over time. Most understand the benefit of a more comprehensive data privacy program but struggle to implement it. Surprisingly, this is not primarily due to a lack of resources, but rather to a lack of maturity in their approach. External partners play a key role helping firms prioritize actions and execute on a holistic data privacy strategy.[211]

Thus, compliance with the new privacy regulations is essential for companies to ensure trustful relationships with consumers.

Technology companies provide many conveniences for free. However, given the nature of the digital market, this concept of free convenience sounds naïve and perhaps unsuitable. Social media, Google, Yahoo, and other innumerable tools are available to users without a monthly or instantaneous payment. How do they work? Are all these commodities free? The answer is no. Companies are using the data generated by users to determine consumers' preferences and sell advertisements for businesses around the world. Through sharing people's personal data,

[209] IBM, Proliferating privacy regulations, https://ibm.co/2HNcyHc (last visited, Feb. 23.2020).
[210] *Id.*
[211] Sophia Christakis, *Data Privacy is the New Strategic Priority*, Forester, 12 (Jul. 2019).

companies move millions and millions of dollars.[212] Therefore, there is some apparent lack of transparency in corporate behavior in disguising the cost of free services to users.

3.1 Facebook

Facebook is one of the most popular social media enterprises in the world. It is an American multinational that involves billions of users because many people have a Facebook account or use one of its apps, such as Message, WhatsApp, and Instagram to send and receive messages.[213] Through Facebook or Instagram, people share practically everything about their lives, such as pictures of parties, houses, vacations, meetings with friends, places of employment, and so on. All of these actions generate a huge amount of data, which is used by the company to earn an incredible revenue. Facebook does not charge users for creating accounts or using the online platform. Through AI, the corporation gives users a personalized experience by providing targeted advertisements based on the data shared. These advertisements match almost exactly with users' preferences. It appears that Facebook has more than 2.6 billion users worldwide,[214] which makes Facebook the perfect place to advertise. Thus, part of the revenue of the company comes from advertisements.

According to Jason Henry, "Facebook's user data extends far beyond the basic biographical information that most share. Facebook also tracks users on other sites and apps, collects so-called biometric facial data, and allows marketers to target people who express an interest in certain

[212] See Jathan Sadowski, *Companies are making money from our personal data –but at what cost? Data appropriation is a form of exploitation because companies use data to create value without providing people with comparable compensation*, The Guardian (Aug.31.2016), https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon

[213] Facebook, *Facebook Brand Resource Center*, https://en.facebookbrand.com/, (last visited Apr.15.2020).

[214] J. Clement, Facebook: Number of monthly active users worldwide 2008-2020, Statista (Apr. 30, 2020), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

health conditions."[215] The company manages the personal data shared on its platform for different purposes besides advertisement without users' authorization. Users expect to have control of their privacy when they share private data, such as an addresses, ages, pictures of family, and opinions about different posts. As such, they do not give third parties the authorization to access their personal data. However, some past experiences show that personal data shared on the platform is exposed and vulnerable to third party access. The questions here are: What is the relationship between Facebook and its users – free access to the platform with the expectation of privacy or with no expectations of any sort? Is there an agreement between Facebook and users, and if so what is in the agreement? Irrespective of whether there is an agreement, should users reasonably expect the protection of their privacy? It appears that in the early stages, Facebook and users did not enter into a contract. Information on how the data would be used was not clear, and it was unclear what users' expectations were with regard to the privacy of data. A clear contract between Facebook and its users raises questions about privacy and vulnerability of the use of data by third parties. These vulnerabilities were brought to light by the Cambridge Analytica scandal, which involves a data breach.

Facebook has been involved in some polemic controversial cases associated with the breach of data. For instance, the Cambridge Analytica scandal revealed that Facebook exposed data on up to 87 million users. These data were in the hands of a researcher who worked for Cambridge Analytical and worked in the Donald Trump campaign. The public became aware of this incident in early 2018.[216] The breach resulted from Facebook's voluntary conduct of giving

[215] Jason Henry for the New York Times, Natasha Singer, *What do Don't Know About How Facebook Uses Your Data*, New York Times (Apr.2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

[216] Alvin Chang, *The Facebook and Cambridge Analytica Scandal, explain with a simple diagram*, Vox (May,2.2018), https://bit.ly/2wKrUdv

access to its data without restrictions. Facebook failed to police the use of that data by Cambridge Analytica. Basically, through a personality test app, Cambridge Analytica also collected information about the test-takers' Facebook friends. The company utilized this type of data to draw a specific advertisement for each group according to their personality, which was linked to the Donald Trump campaign. The company claims it was responsible for the election of the President using data to target people, although this could not be proved. Facebook, through the FBLearner Flow, uses machine learning to analyze all data shared by users.[217]

Moreover, AI facilitates the collection and storage of data, showing that corporations are vulnerable. The protection provided to Facebook users was not adequate since Cambridge Analytica is an example of how shared data can be used in different ways.[218]

In the same year, Facebook faced another data breach in Europe, exposing 3 million users' personal information, and another 30 million people worldwide had their Facebook data exposed. Again, the trustful relationship between users and Facebook was exposed and weakened. These examples illustrate some of the vulnerabilities the company faces when protecting the privacy of users. Questions include the following: What is the company doing to prevent these accidents and to comply with the new data protection law? Can AI technology help in this process?

Therefore, in order to operate its platform in the EU cyberspace, Facebook prepared products and services to comply with the GDPR.[219] In the U.S., one of the strongest laws is the CCPA, which has been compared to the GDPR. Facebook alleges that it does not need to change

[217] MARR ET AL., *supra* note 60 at. ch.6.
[218] Alvin Chang, *The Facebook and Cambridge Analytica Scandal, explain with a simple diagram,* Vox (May,2.2018), https://bit.ly/2wKrUdv
[219] Facebook Business, *Facebook's commitment to data protection and privacy in compliance with the GDPR* (Jan.29.2018). https://bit.ly/2HT38tY

anything in its service since the company does not sell data, so the CCPA would likely not apply to Facebook.

However, Scott Ikeda argues,

> The catch that Facebook thinks will get them out of CCPA is that businesses are able to install Pixel free of charge, and pay only for Facebook to deliver targeted ads based on the information they harvest. Facebook believes that they are excepted from the CCPA terms given that they are not directly selling the personal data they collect to these businesses, and given that it is never made visible to them. The business simply provides Facebook with the general demographics to target ads to, things like location and age range, and Facebook targets their ads to users it believes fit the requested profile.[220]

In the U.S., there is some friction between the requirements of the law and business purposes. The question is whether the act of sharing personal data with businesses and creating direct advertisements using this data are selling transactions, since the companies pay for the advertisements generated by the shared data. The data protection laws are new, and new guidelines and clarity are necessary to require transparency from corporations. The company promises to use AI advances to promote a safe social media platform. For instance, Facebook recently launched an AI tool to detect posts where a user imitates images or videos without their consent. Thus, before anyone can have access to those images, the tool can detect them.[221] The use of AI to improve safety in online platforms will help corporations build a stable relationship with users.

Regardless of privacy protection and AI, Facebook has set a series of innovations on privacy ambiance, making users responsible for their shared data. The corporation provides these settings through Privacy Checkup. Another innovation is the possibility that users can administrate the ads they want to see through the platform. However, users wonder, "How does Facebook

[220] Scott Ikeda, *Facebook refuses to Change Web Tracking Practices, Believes That CCPA Does Not Apply to Them, CPO Magazine* (Jan.06.2020). https://bit.ly/3a2Qm88
[221] James Vincent, *Facebook promises new AI tool will proactively detect revenge porn*, The Verge (Mar.15.2019) https://www.theverge.com/2019/3/15/18266974/facebook-instagram-revenge-porn-ai-filter

decide which ads to show me?" Facebook also permits users to control or disconnect the information sent to Facebook about their activity on other websites and apps. Although the company has adopted these settings, they assert they do not sell data and believe that what a person shares and with whom they share it should be the user's decision. All data stored on Facebook devices, such as a Facebook app, Messenger, Instagram, and WhatsApp have been used to train machine learning in several corporations' new projects.[222] One of these projects is facial recognition, which operates based on database photos that identify key features, such as distance between the eyes, mouth size, and other facial characteristics that make each person unique. However, the question here is whether the right of anonymity to not have the face revealed is respected and whether the use of personal data shared with friends with specific purposes can be used for other purposes. There are no federal regulations to control the use of this technology.

3.2 Alphabet and Google

Alphabet is a multinational technology including life-science and Internet services. Its business includes Google, life-sciences company Verily, self-driving technology Waymo, smart home device Nest, and Deep Mind between others.[223] Through the Google search engine, these companies are exploiting AI in different fields. The corporation also creates the idea that the service the search engine provides is free. However, considering the data users generate and how this data raises revenue for the company, it seems consumers are exchanging personal data for the services provided. Google's search does what its name suggests: It permits anybody who is not

[222] Facebook, *We are committed to honoring your privacy choices and protecting your information*, https://about.fb.com/actions/protecting-privacy-and-security/(last visited 20.03.2020).

[223] MARR ET AL., *supra* note 60 at. ch.2.

specifically a customer to search for any information on the Internet. The search engines facilitate the discovery, organization, recovery, and storage for the user.[224] What is retrieved is neither posted by Google nor on Google's website. The activity involves mostly third parties with Google as the facilitator. On the other hand, Google tracks every single search a person makes when using the search engine. It does not matter if the person uses the search engine in text, image, or voice. Through an algorithm called Rankbrain, introduced in 2015,[225] the company generates revenue by offering space for ads in its platform. The advertisements are directed at people according to their search preferences. This marketing technique makes Google one of the most useful and efficient place for companies to advertise.[226] However, the question posed here is whether content posted by third parties found in the Google search exposes Google to the requirements for the protection to privacy and fundamental rights protection.

A case between Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González known as *Google Spain v. Costeja Gonzalez*[227] shows that privacy is a fundamental right, the right to be forgotten, and the extraterritorial reach of EU law on Google's parent company. Mr. Gonzalez requested the newspaper to erase his name from publications and Google to remove his personal information from the search results it provides to its users. The Spanish Data Protection Authority dismissed the request related to the newspaper but approved it in relation to Google. The court found that search engines are personal data processors based on the EU Directive 1995/46/EC.[228]

[224] Neil Patel, *How Google's Search Engine Really Works* (A Peek Under the Hood), https://neilpatel.com/blog/how-google-search-engine-really-works/ (last visited May, 3 2020).
[225] MARR ET AL., *supra* note 60 at. ch.2.
[226] Jerry Hildenbrand, *Does Google sell your personal Data? The short answer: no. It's valuable to them if they keep it for themselves* (Jan. 2018), https://www.androidcentral.com/does-google-sell-your-data
[227] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014 ECLI: EU: C: 2014:317 [hereinafter Google Spain SL v. AEPD].
[228] DIRECTIVE(EU) 95/46/EC, 1995 O.J. (L 281/31-50).

Afterward, Google Spain and Google Inc appealed to the High Court of Spain. But, before analyzing it, the High Court of Spain submitted it to the Court of Justice of the European Union (CJEU),[229] seeking guidance whether Google was subject to the notion of a processor of personal data and also whether Google U.S., the parent company of Google Spain, needed to comply with the directive provisions. And in case of a negative answer, it was requested that the CJEU determine Google's liability as a data processor and evaluate whether a citizen has the right to require Google to delete his personal information, which is known as the right to be forgotten. The CJEU after a detailed analysis concluded that Google is a processor of personal data; it "'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results."[230] Thus, under Article 2(b) of the Directive 95/46, Google was classified as a processor. The court also concluded that Goggle Spain was an affiliate of Google Inc since "according to the referring court, the promotion and sale of advertising space, which Google Spain attends to in respect of Spain, constitutes the bulk of the Google group's commercial activity and may be regarded as closely linked to Google Search."[231]

See Konstantinos Kakavoulis, *The Case Google Spain v AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A brief critical analysis* (Jun. 20.2018), https://www.homodigitalis.gr/en/posts/2900
See also *The right to be forgotten (Google v. Spain)*, epic.org, https://epic.org/privacy/right-to-be-forgotten/
See David J. Stute, *Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD*, 36 Michigan Journal of International Law, issue 4, 650 (2015).

[229] "Since the establishment of the Court of Justice of the European Union in 1952, its mission has been to ensure that 'the law is observed' 'in the interpretation and application' of the Treaties.
As part of that mission, the Court of Justice of the European Union: reviews the legality of the acts of the institutions of the European Union, ensures that the Member States comply with obligations under the Treaties, and interprets European Union law at the request of the national courts and tribunals."
Court of Justice of the European Union , General presentation,
(CJEU), https://curia.europa.eu/jcms/jcms/Jo2_6999/en/ (last visited May.4.2020). The Treaty on the Functioning of the European Union (TFEU), Article 256 authorizes the CJEU to review cases decisions from the EU Member States. See Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012 (326/159).

[230] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014 ECLI: EU: C: 2014:317, 10 [hereinafter Google Spain SL v. AEPD].

[231] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014 ECLI: EU: C: 2014:317, 13 [hereinafter Google Spain SL v. AEPD].

As a result, Google Inc is subject to the EU directive. The CJEU found that the search engine has the right to process personal information when it is a justifiable interest of the data holder or third party to be served. Nonetheless, this right is not absolute when applying it to fundamental rights. The data holder finds some limitations, specifically in its right to privacy. Thus, the court highlights that the economic interests of the search engine cannot surpass or create a limitation to the right to privacy. Regardless of this, the court found that Mr. Mario Costeja Gonzalez had the right to have his personal data erased from Google. Therefore, this decision is considered an important precedent to the "right to be forgotten" for data subjects addressing to the controller pertinent obligation.[232]

In 2018, Google Plus exposed the data of 500,000 people, including names, emails, and occupations. Nonetheless, the company did not inform users until the Wall Street Journal published the story. Then, in December 2018, 52.5 million Google Plus users had their data breached, and again, the company did not give notice of the breach in the time required to inform users.[233] Under Article 33 of the GDPR,[234] the company has 72 hours to notify users about a breach and risks to which they are exposed. Nonetheless, the 2018 Google incident was covered by top executives to keep the company out of government regulation; to justify their actions, the company explained that they did not disclose the incident because they could not accurately identify the users.[235]

The U.S., as explained earlier, does not have one federal regulation that covers data protection in all sectors. Thus, companies comply with state laws that require them to notify users but do not have specific terms. On the other hand, under the CSL Article 42, in case of a data

[232] Konstantinos Kakavoulis, *The Case Google Spain v AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A brief critical analysis* (Jun. 20.2018), https://www.homodigitalis.gr/en/posts/2900
[233] Michael Grothaus, *How our data got hacked, scandalized, and abused in 2018*, (Dec.13.2020), https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018
[234] See REGULATION (EU) (GDPR) 2016/679, art. 33, 2016 O.J. (L 119/52).
[235] Sara Salinas, *A Google bug exposed the information of up to 500,000 users*, (Oct. 8.2018), https://www.cnbc.com/2018/10/08/google-bug-exposed-the-information-of-up-to-500000-users.html

breach, the operator needs to report possible disclosure of the network to the competent authority and take immediate remedial steps. [236]

Thus, Google has great responsibilities related to the use of personal information on AI projects, since the corporation is exploiting many AI innovations. The company presents a set of steps they consider when using data collected through the search engine to create more AI innovations based on fairness, interpretability, privacy, and security. Furthermore, the company presents some concerns about the use of sensitive data in machine learning and how to provide adequate transparency. In addition, the company does not present a solution for this concern, but gives assurances that they are working to find trustful solutions and to comply with the laws.[237] However, the company does not feature any solution for the constant surveillance and indiscriminate use of personal data. The question here is whether the benefits offered by Google are enough to keep "the right to be let alone,"[238] and why people have personal data shared for many purposes that they do not know anything about. Of course, fairness and transparency are key elements to building a trustful relationship between society and a company. Nonetheless, fairness and transparency do not supplant the right to anonymity and liberty. In 2019, Google broadcasted that TensorFlow Privacy safeguarded users' data with a technique known as different privacy.[239] Thereby, the company uses this technique to comply with the laws and is seeking to prove that users can trust the platform.

[236] King & Wood Mallesons et al., *China: Data Protection 2019*, ICLG (Mar. 07.2019), https://iclg.com/practice-areas/data-protection-laws-and-regulations/china
[237] Google AI, *Responsible AI Practices*, Google, https://ai.google/responsibilities/responsible-ai-practices/?category=privacy, (last visited Mar.20.2020).
[238] Warren and Brandeis, *supra* note 4.
[239] James Vincent, *Google is making it easier for AI developers to keep user's data private,* The Verge (Mar.6.2019), https://bit.ly/3av1g6Y

3.3. Amazon

Jeff Bezos founded Amazon in 1994 as an online book store. However, the visionary Bezos saw more potential than the simple act of selling books online. Bezos wanted the online book store to become a giant technology company that provides various services, including retail, and it eventually expanded into house technology surveillance products. The way the company manages personal data to achieve these goals is astonishing. According to Bernard Marr et al.,

> Today, Amazon is a multinational e-commerce giant and the world's leading cloud computing provider, making it the third most valuable public company in the United States. Beyond its core retail and cloud business, the company also has a publishing business, a film and television studio operation, and produces consumer products such as the Kindle e-readers, Fire tablets and TV sticks, as well as the Amazon Echo.[240]

Thus, the company achieved domination in several sectors. The question is how Amazon does it. How can the company predict the next time a consumer will buy something? How does it know what the purchaser should buy? Does the convenience surpass the surveillance? These questions and others keep Amazon at the top of the list for evil companies.[241] Amazon is based on data collection and AI tools.

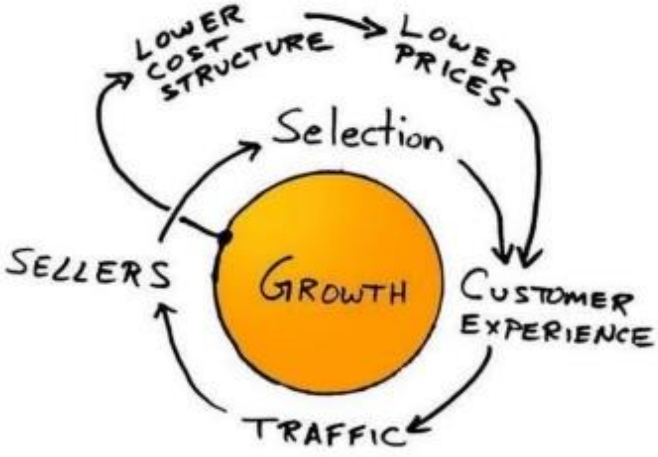
Through the collection of data, the corporation tracks consumers' behavior, combining this information with products that match the purchaser’s preferences or others that the machine indicates as similar and can be added to the buyers' predilection. This is known as deep learning, and it is designed to provide users with personalized shopping experiences, where a user has access to data from the last purchase, including items bought and recommendations.[242]

[240] MARR ET AL., *supra* note 60 at. ch.3.

[241] *The Evil list Which tech companies are really doing the most harm? Here are the 30 most dangerous, ranked by the people who know,* Slate, technology (Jan.15.2020), https://slate.com/technology/2020/01/evil-list-tech-companies-dangerous-amazon-facebook-google-palantir.html

[242] MARR ET AL., *supra* note 60 at. ch.3.

Nonetheless, Amazon is seeking to go beyond online relationships with consumers. In 2015, Google launched Alexa, a device capable of executing home tasks. Everything that was in the movies became true: The ability to control the house through voice commands converted into reality with deep learning and its natural language algorithms.[243] Amazon has also been spreading AI through "flywheel,"[244] using growth and massive scale to enhance the customer experience through low prices. Below is an illustration of Amazon's business.



The Virtuous Cycle, as drawn by Amazon.

Figure 3. Amazon Virtuous Cycle.[245]

Moreover, leading technology companies collect personal data to be used in the machine learning process to discover patterns to make better decisions on behalf of consumers. The corporation gives assurance that personal data is protected through state-of-art privacy-enhancement, which is a set of company-wide processes and policies that govern all data processed

[243] MARR ET AL., *supra* note 60 at. ch.3.

[244] See more about Amazon Flywheel, *Sam Seely*, *The Amazon flywheel: part 1*, (May. 02.2016), http://www.samseely.com/blog/2016/5/2/the-amazon-flywheel-part-1

[245] *Sam Seely*, *The Amazon flywheel: part 1*, (May. 02.2016), http://www.samseely.com/blog/2016/5/2/the-amazon-flywheel-part-1

and stored in Amazon systems. The data handling policies specify the use of cryptography that restrict access to the data. In the context of machine learning, the corporation justifies that the system does not memorize any specific individual in the dataset, but they also do not explain how this is possible.[246] However, the company uses patterns of a fraction of the population. Therefore, individual privacy is safeguarded in the sense that the company does not use sensitive data. On the other hand, the data used to separate groups of patterns are a risk, taking into consideration that the company uses these pieces of information for other purposes, which can target a part of a city. The question is whether, as a group, the right of privacy is changed. The "right to be let alone" is flexible when targeting specific groups of society. When the system does not use names and social security numbers, known as sensitive data, does the data lose personification? Is the use of gender, age, and location not personal data? The flexibility to collect data and manipulate it for different purposes endangers privacy.[247] Indeed, this combination of AI and Amazon is what keeps the company in the list of top e-commerce corporations. Nevertheless, the question is whether all this technology also interferes with individuals' privacy. It is not a secret that Amazon workers face a dangerous labor environment and are treated as robots where speed is more important than breathing, depending on the function.[248] But, besides that, through the collection of personal data, the giant corporation has shown how harmful the act of sharing data can be to society. For example,

[246] Day One Staff, *Amazon AI Protecting data privacy: How Amazon is advancing privacy-aware data processing* (Jul.09.2018), https://blog.aboutamazon.com/amazon-ai/protecting-data-privacy

[247] See Latanya Sweeney, *k-anonymity: A model for Protecting Privacy*. 10 Int. J. Uncertain. Fuzziness Knowl.-Based Syst., 558 (2002).

[248] See Will Evans, *Ruthless Quotas at Amazon Are Maiming Employees his holiday season, Amazon will move millions of packages at dizzying speed. Internal injury reports suggest all that convenience is coming at the expense of worker safety*, The Atlantic (Dec. 5.2019), https://bit.ly/2TYlHUq
See Michael Sainato, *'I'm not a robot': Amazon workers condemn unsafe, grueling conditions at warehouse,* The guardian (Feb. 5.2020), https://bit.ly/33sI9Ip
See Eric Spitznagel, *Inside the hellish workday of an Amazon warehouse employee*, New York Post (Jul.13.2020), https://bit.ly/33zL563

with the police supported surveillance Ring doorbell,[249] everything people do is recorded and can be required from the police to solve crimes. On the other hand, Amazon is proposing to apply face recognition to advance the Ring doorbell system, which complicates the task, since the test proved that the system could misidentify black people. This system could increase rates of crimes, discrimination, and so on.[250] The question is whether the right to be let alone will prevail with cameras everywhere. Morgan G. Ames states other behaviors and inventions with which Amazon is involved:

> 1. Racked up a massive carbon footprint with rapid shipping as well as AWS cloud-based computing;
> 2. Contributed tech to military and intelligence agencies with dubious human rights records, including U.S. Customs and Border Protection operations separating families at our own border;
> 3. Failed to moderate what is on its platform, resulting in a glut of dangerous fakes such as easily broken counterfeit car seats for children.[251]

These are some examples of how the indiscriminate gathering of personal data can be harmful. Consumers trust companies when making simple purchases and sharing their data. However, the corporation manipulates it without any concern, aiming for profit. The question is whether the sharing of personal data with the police department and other government agencies is an invasion of privacy and whether someone has the right to keep family and personal beliefs protected. It seems that, in the digital era, corporations and governments are trying to make the concept of

[249] See Alfred Ng, *Amazon's helping police build a surveillance network with Ring doorbells,* Its popular Ring smart doorbells mean more cameras on more doorsteps, where surveillance footage used to be rare, Cnet (Jun.5.2019), https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/

[250] See Lauren Goode, *Amazon Doubles Down on Ring Partnerships with Law Enforcement the Company's top Hardware executive told Wired he's "proud" of the controversial program and hinted at a future with more facial recognition (Jan.07.2020),* https://www.wired.com/story/ces-2020-amazon-defends-ring-police-partnerships/

[251] Morgan G. Ames, *The Evil list which tech companies are really doing the most harm? Here are the 30 most dangerous, ranked by the people who know,* Slate, technology (Jan.15.2020), https://slate.com/technology/2020/01/evil-list-tech-companies-dangerous-amazon-facebook-google-palantir.html

privacy as a fundamental right less rigid to achieve purposes such as security and the needs of society. [252]

The business model used by the three tech multinationals has always preceded the law. Although the right of privacy goes all the way back to the common law, the protection of privacy has remained a challenge, particularly in the modern AI era. Tech multinationals precede existing laws on privacy and fundamental rights as the companies expand technologically into face recognition, voice, biometric personal information, and other forms of technology to be discovered. The question is whether existing laws will be sufficient to protect privacy, data, and fundamental rights. It appears that some reliance has to be placed on the companies to design systems to protect these rights, even when the law is deficient.

[252] J. Van den Hoven et al., *Privacy and information Technology,* Metaphysics Research Lab, Stanford University (Winter, 2019).

CHAPTER 4: ARTIFICIAL INTELLIGENCE AND DATA OWNERSHIP

Since AI’s use of big data is a key point for machine learning, data ownership has a direct impact on AI. The different types of data raise the question of who owns the data. Is it the one who generates the data when she uses different platforms, or is it the service providers? For instance, when a person navigates through the Internet using the Google search engine, Google has cookies that follow users and collect data about them and the users do not know they are been followed. Who owns that data? Besides the issue of ownership, a further question is whether the users can maintain control of the data collected. An analysis of Facebook’s platform raises the question of whether users have the power to control their privacy settings, and who owns the data. Can this type of conduct be interpreted as the users giving away their data ownership? In this case, would the data be shared with third parties? Who would not be a problem for Facebook? In situations where the company sanitizes the data, deleting sensitive data such as name, age, and address, but using the data to target groups, who owns this data? Is it the group of people included in the data or the company responsible for the sanitization of the data? These seem to be important questions when one thinks about data ownership. However, the strengthening of regulations related to data protection cannot be considered a barrier to AI advancement. New regulations have required that corporations need to give clear information to clients when using personal data. It means information on the business purpose of using the personal data, how the data is managed, and for how long the data will be stored should be clear. Thus, the company needs permission from consumers or users in order to manipulate their personal data. According to Jan Feuerhake,

> Within the European Union, there is no coherent approach on ownership of data as such. Restrictions of usage and disclosure of data other than personal data mainly stem from contractual relationships. Developers of artificial intelligence tools and

> users will have to bear in mind closely what they want to do with data and what the respective contracts allow.[253]

Thus, where the law does not say what can be done, corporations will regulate ownership through contracts, and the main point is the required authorization from clients to use data.

4.1 Impact of AI on Society.

The impact of AI on society, and on the next generation, will be enormous. The present generation is experiencing an adaptation phase and the next generation will be immersed by AI. Some governments have started to prevent the impact of AI by implementing strategies. In 2016, the Executive Office of President Obama developed a document on artificial intelligence, automation, and the economy. The document brings important considerations about AI and the economics of AI-driven automation:

> AI raises many new policy questions, which should be continued topics for discussion and consideration by future Administrations, Congress, the private sector, academia, and the public. Continued engagement among government, industry, technical and policy experts and the public should play an important role in moving the Nation toward policies that create broadly shared prosperity, unlock the creative potential of American companies and workers, and ensure America's continued leadership in the creation and use of AI.[254]

Notwithstanding the claims of this document, the policies and laws will be drawn according to outcomes, such as unemployment, replacement of humans by machines, and so on. Technological advances are inevitable, and the mission to make this process less painful and more beneficial is in the hands of each government around the world. The Executive Office of President Obama's document focuses on economic impact and how it can be addressed. It also points out that many

[253] Jan Feuerhake, LL.M., AI, data protection and data ownership, https://iot.taylorwessing.com/ai-data-protection-and-data-ownership/ (last visited, Feb.07.2020).
[254] Executive Office of the President Obama, *Artificial Intelligence, Autonomy, and the Economy* 4 (Dec. 2016).

jobs will be replaced and policymakers will play an important role in drafting policies to help people be trained or learn new techniques to return to the job market again. The document also indicates,

> Today, it may be challenging to predict exactly which jobs will be most immediately affected by AI-driven automation. Because AI is not a single technology, but rather a collection of technologies that are applied to specific tasks, the effects of AI will be felt unevenly through the economy. Some work tasks will be more easily automated than others, and some jobs will be affected more than others. [255]

It seems the question will always be whether a transition to job automation is necessary and when this automation will start. Technological advances and AI drive people's lives, and most of the time, this impact is imperceptible. Perhaps a plan showing how many functions will be replaced and how to transfer those people to other positions or other jobs is the rational way to approach the issue and prevent an abrupt transition.[256]

Some scholars allege that it is too early to draft regulations. On the other hand, information privacy needs to be insulated from any interference now to safeguard the right to have personal data preserved and protected. Perhaps it is not early to think about responsibility, liability, mass unemployment, and what the new tools are putting in danger.

Jack Ma Alibaba, Cofounder of the World AI Conference in Shanghai, clarified some questions about AI and the implications for humanity. He affirms,

> I'm happy about the artificial intelligence, or Alibaba intelligence, that's going to understand a human, the inside of the human, better. So when people worry a lot about artificial intelligence, people should have more confidence in themselves. Because I think a lot of solutions we don't have today, but there will be solutions tomorrow. [257]

[255] Executive Office of the President Obama, *Artificial Intelligence, Autonomy, and the Economy* 13 (Dec. 2016).

[256] See James Manyika et al., Jobs Lost, Jobs Gained, Workforce Transitions in a time of Automation, Mckinsey Global Institute, (Dec.2017), see also Calum McClealland, *The Impact of Artificial Intelligence- Widespread Job Losses*, iot for all (Jan.15.2020), https://www.iotforall.com/impact-of-artificial-intelligence-job-losses/

[257] Ricki Harris, *Elon Musk: Humanity Is a Kind of 'Biological Boot Loader'for AI,* Wired (Sep.01.2019). https://www.wired.com/story/elon-musk-humanity-biological-boot-loader-ai/

It is an optimistic point of view, and he does not see AI as a replacement of humans. In other words, he believes that AI will help to better understand humans. He also asserts an essential view that education needs to move on. Kids need to be prepared, to be creative, and learn things that these machines still cannot do.

Society is moving into a new era. Preparing humanity to move forward and work in harmony with this technology is a crucial point. Most of these new machines are playing an important role around the world and helping humans find solutions to problems in a faster way or executing tasks that before needed more people to execute. Of course, these transformations can be harmful if governments do not prepare society for the outcome.[258] For instance, Nick Bostrom, when questioned about the impact that AI will cause on the job market and economics, argues,

> In the very short term, I think that there might be a tendency to exaggerate the impacts on the labor market. It is going to take time to really roll out systems on a large enough scale to have a big impact. Over time, though, I do think that advances in machine learning will have an increasingly large impact on human labor markets and if you fully succeed with artificial intelligence, then yes, artificial intelligence could basically do everything. In some respects, the ultimate goal is full unemployment. The reason why we do technology, and why we do automation is so that we don't have to put in so much effort to achieve a given outcome. You can do more with less, and that's the gestalt of technology.[259]

It seems to be wise to develop plans for the transition. As stated in the Obama executive plan, a transition plan such as training workers to execute new functions, because machine will be doing their jobs, in a short time will be necessary. Perhaps the best way to prevent a clash between technology and humans is to find a balance between common sense and regulations. The impact of AI on society will be disastrous if the process is not limited through laws and forecasts to permit the transition to jobs and learning processes. It is time to transform all human learning processes

[258] Nick Bostrom is a professor of Oxford and Director of the Future of Humanity Institute. For more information see https://nickbostrom.com/ (last visited, Feb.02.2020).

[259] MARTIN FORD, ARCHITECTS OF INTELLIGENCE: THE TRUTH ABOUT AI FROM THE PEOPLE BUILDING IT, ch.5 (Packt Publishing, 2018).

to harmonize society. In spite of this, the impact of AI on society will vary, depending on what AI is used for.

4.2 Benefits and Risks of Data Protection and Artificial Intelligence

The benefits that AI brings are innumerable. For instance, AI is used to execute simple functions in a mobile phone, to complete or offer auxiliary support in complex tasks such as cancer diagnoses and surgeries, and to operate production with advanced autonomous control. AI innovations are a reality that is increasing, revolutionizing, and improving the world. AI has been in disaster areas to identify survivors through algorithms and to survey aerial footage. Credit card companies are using AI to identify and strike fraud.[260] In medical uses, AI has been a faster and more accurate resource in cancer diagnosis.[261] So, these are just a few examples of AI benefits, and in the near-future, AI will be able to achieve more difficult tasks in several areas.

However, these benefits also endanger data protection. AI depends on data to learn, execute, and manage tasks. Perhaps the best way to properly regulate AI is to place limitations and barriers to any system with bias, autonomous killing machines, indiscriminate surveillance without individuals' permission, and other ways that AI can harm humanity. The regulation may involve strict policies to punish businesses, developers, and researchers enrolled in these types of AI. Here, the importance of a global law that applies to all countries about forbidding the use of AI would prevent anyone from pursuing the projects listed above. That is what the United Nations Institute

[260] Amitai Etzioni et al. *Artificial Intelligence Be Regulated?* 4 Issues in Science and Technology 32 No.4 (Summer 2017).

[261] Fergus Walsh, *AI' outperforms' doctors diagnosing breast cancer*, BBC News (Jan.2.2020), https://www.bbc.com/news/health-50857759. This article explain how Google Heath and Imperial College London are implementing AI in the cancer diagnosis and how it can save lives.

for Disarmament Research (UNIDIR) has been discussing since 2014, through the "Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward."[262]Another important document is the open letter announced on July 28, 2015, at the International Joint Conference on Artificial Intelligence (IJCAI).[263] It is also the government's responsibility to protect society by taking action to find ways to suppress harmful outcomes related to AI, in weaponization and job replacement, and doing what is necessary for AI to provide general welfare. Since AI systems rely on human input, machines cannot survive without humans. Thus, the control of what AI can or cannot do is in human hands.[264]

Therefore, regulations protecting data have a direct effect on AI developments since accuracy depends on the amount of data to which the machine is exposed. Taking an overview of the three legal systems' data protection regulations, the GDPR inhibits the use of personal data without consent and limits it in many ways, including the way that companies store data. The GDPR provides protection for EU citizens, giving them the right to privacy. On the other hand, it can prevent them from enjoying the benefits of AI. Thus, the GDPR has not yet achieved the correct balance between regulation and the benefits of AI advances.

[262] UNIDIR, *Weaponization of Increasingly Autonomous Technologies: Considering how Meaningful Human Control might move the discussion forward*, 12 UNIDIR Resources (Nov.13.2014)." An attempt to develop national or international norms to address the challenges associated by the weaponization of increasingly autonomous technologies will need organizing principles that can be understood and broadly shared by a variety of States, civil society organizations, the public and the media." This document has important concepts and ideas how the weaponization can be controlled.

[263] Future of Life Institute, *Autonomous Weapons: An Open Letter From AI & Robotic Researchers*, https://futureoflife.org/open-letter-autonomous-weapons/ (last visited Apr.15.2020). In this website it is possible to see the name of the endorsers and AI/ Robotics Researchers. See also Samuel Gibbs, *Elon Musk leads 116 experts calling for outright ban of killer robots*, The Guardian, (Aug.20.2017),https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war

[264] See Amitai Etzioni et al., *supra* note 260.

The set of laws in the U.S. protects data sectored, but are not as restrictive as the CCPA. The U.S. wants to be a leader in AI discoveries and implementation. President Donald Trump undoubtedly stated this goal in the Executive Order on Maintaining American Leadership in AI. The Executive Order stated several objectives to be achieved. The first objective is to promote sustained investment in AI research and development (R&D) in collaboration with industry, academia, and international partners. The second objective focuses on enhancing access to high quality and traceable federal data while maintaining security, privacy, safety, and confidentiality. The third objective focuses on reducing barriers to the use of AI technologies and promoting their innovative application. The fourth objective raises the importance of ensuring technical standards to minimize vulnerabilities to attacks from malicious actors. The Executive Order also aims to train the next generation of American AI researchers and to ensure the development and implementation of the action plan under the National Security Presidential Memorandum of February 11, 2019.[265]

China seeks to lead AI discoveries by investing in the monopoly of data which creates a favorable environment for national companies. On the other hand, China also sets strong punishments for companies, operators, and networks that break the law, thereby creating a trustful atmosphere for consumers. However, none of the data protection laws are in equilibrium with AI. To achieve equilibrium, constant guidelines, amendments, and revisions are necessary.

According to Fred H. Cate and Rachel Dockery,

> Many regulators, businesses, attorneys, and academics are working hard to find ways to address the challenges presented by AI to data protection laws. These are important initiatives and obviously necessary in light of the urgent need for users of data to comply with existing data protection laws. However, as we have seen, the tension between those laws and AI is so great and so fundamental that efforts to reconcile them run the risk of weakening data protection or interfering with the

[265] European Commission, *Policy Artificial Intelligence*, Digital Single Market, https://ec.europa.eu/digital-single-market/en/artIificial-intelligence (last update Dec. 09.219).

> benefits of AI. Neither result is desirable given the importance of AI and of personal privacy.[266]

It is of fundamental importance that legislators find the correct balance to guarantee the protection of personal data to society so that companies can pursue the exploitation of new AI innovations. In addition, AI developers need to do more than comply with laws, and improve ways to provide transparency, accuracy, and security. If people know what companies do with their data and the benefits of these actions, this may facilitate the use of personal data because people can trust corporations when using personal data. Everything will depend on the purpose and risks related to it. The question will always be whether a person can trust automated decisions. Corporations need to disclose how the system works by informing society, and governments need to ensure that the information disclosed by companies will not be stolen when disclosed. Hence, all limitations of data protection imposed on AI developers do not solve the issues, because the data flow is an essential point to AI.[267]

The three legal systems discussed do not have specific laws devoted to AI and data protection. However, as stated in previous sections, the EU, China, and the U.S. are adapting their old laws to attend to the demands of AI. As an example, the EU launched a European strategy for data. The EU Commission argues that,

> The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. It should be a space where EU law can be enforced effectively, and where

[266] Fred H. Cate & Rachel Dockery, *Artificial Intelligence and Data Protection: Observations on a Growing Conflict, Ostrom Workshop*, 18 *(2019).* https://ostromworkshop.indiana.edu/pdf/seriespapers/2019spr-colloq/cate-paper.pdf

[267] See Frank Pasquale, *Data-Informed Duties in AI Development*, 119 Colum. L. Rev.1917-1940(Nov. 2019). Pasquale argues that: "Law should help direct—and not merely constrain—the development of artificial intelligence (AI). One path to influence is the development of standards of care both supplemented and informed by rigorous regulatory guidance." Which is the same idea this paper defends. It is necessary laws that not barrier AI developments, but find a correct balance between regulations and innovations.

> all data-driven products and services comply with the relevant norms of the EU's single market.[268]

The EU strategy indicates the efforts countries are making to retain the benefits of AI without losing privacy. The EU Commission's communication in its new strategy calls for harmonization and feedback between the EU member states. The document points out that society generates data, and this data needs to be used for society's benefit. For instance, data can combat emergencies, improve public services, help to forecast climate change, and so on.[269] Thus, the approach of strict laws is not the appropriate way to solve conflicts between AI and data protection since the benefits of AI and data are innumerable. On the other hand, implementing regulations with severe punishments for bias, discriminatory programs, machine mistakes, and everything else that can harm society is appropriate behavior. Governments should draft laws to forbid any type of AI that disrupts the general welfare of the public. If the corporation cannot explain to the public what it does with the collected data and the purpose, the project should not be allowed. The balance between economic factors, AI, and privacy needs to be defined since trust is what will allow future AI advances.

[268] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, 4*(Feb.19.2020), https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

[269] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, 6* (Feb.19.2020). https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

4.3 The Scope of Data Protection Regulation in the AI Context: Personal Data

The GDPR states the following principles related to the processing of personal data: Article 5 (a) "Personal data shall be: 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."[270] So, a corporation that uses personal data must manage the operation lawfully, honestly according to Article 6, and clearly demonstrate how the data is being used.

AI is part of people's lives, and the harmonization between AI innovations and privacy principles are essential for an organized society where important principles are respected. Kari Gimmingsrud argues,

> The development of AI is largely driven by economic and societal needs, and development is taking place in virtually all areas of business and society. Data systems and machines can carry out advanced tasks more quickly and at a lower cost. In some areas, AI will modestly challenge privacy principles, while in others it may be perceived as more wide-ranging and problematic, for example if police and judicial authorities use AI as a tool to make decisions, pass judgments, or predict criminal behavior. Or when the health care system uses AI to determine utility and eligibility for treatment.[271]

Therefore, it appears that AI may affect many important fields. How to prevent machines from committing errors and also manage privacy is a challenging question. AI tools also raise issues such as when machines do not make errors, but humans do. Can the users of AI's data-driven conclusions place the blame on the machines? What if the burden is put on the subjects to analyze the conclusions before use or be held legally responsible for errors? David Winter explains that AI errors are more predictable since machines are systematic and their behaviors can be modeled; however, this does not happen to humans. The author concludes that if machine errors can be

[270] REGULATION (EU) (GDPR) 2016/679, art. 5, 2016 O.J. (L 119/35).
[271] Kari Gimmingsrud, *Artificial Intelligence and Data Privacy* , Expert Guides (Aug.20.2019), https://www.expertguides.com/articles/artificial-intelligence-and-data-privacy/aruywukr

predictable, it means they can be easily fixed.[272] Nonetheless, the definition of responsibility still remains in the hands of the programmer or owner who chooses the type of data that influences the machine decision. Machines learn from humans' previous experiences, and the input depends on human actions. As a result, humans can be found responsible for machines' wrong decisions.

Besides these questions, the number of benefits that AI brings must be balanced against privacy principles. Trustful relationships between private companies, governments, and populations are imperative since AI development is directly dependent on data. The GDPR is entirely devoted to rules to protect the "free movement of personal data."[273] Moreover, Articles 12 to 15 of the GDPR state the requirements for transparency. In addition, Article 22 in Chapter 3 seems to be directly connected to AI. Article 22 states the following:

> Automated individual decision making, including profiling, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Paragraph 1 shall not apply if the decision: is necessary for entering into, or performance of, a contract between the data subject and a data controller.[274]

From the article, it can be inferred that a person has the right to inquire and to have the process reviewed when it comes from a machine making decisions based on a specific type of data. Regardless of Article 22, Gimmingsrud offers an explanation:

> An expressed concern with advanced AI is that one does not always know how the result is produced, often called "the black box problem". We can distinguish between two main types of black box problems: 1) Access to algorithms and the logic of the system is deliberately limited by commercial considerations, national security, etc. 2) The system's structure and the algorithm are complicated and difficult to explain. This may be the case, for example, in so-called "neural networks". Non-guided learning also allows systems to identify new patterns and relationships in data that may be difficult to explain.[275]

[272] David Winter, AI Errors vs. Human Errors, International Director (Jun.19.2018), https://internationaldirector.com/technology/ai-errors-vs-human-errors/
[273] REGULATION (EU) (GDPR) 2016/679, 2016 O.J. (L 119/39-43).
[274] REGULATION (EU) (GDPR) 2016/679, art. 22, 2016 O.J. (L 119/32).
[275] See Gimmingsrud, *supra* note 271.

Therefore, understanding how decision-making works is crucial to the trust of the machinery process. Companies will need to find a way to explain how the system works in order to use personal data, which is an advanced approach addressed in the GDPR.

The European Commission in April 2019 prompted the Communication on Building Trust in Human-Centric Artificial Intelligence by highlighting seven key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discriminatory and fairness, societal and environmental well-being and accountability.[276] According to the Commission, to work with these requirements, the GDPR guideline presents an assessment list that helps businesses understand how to apply these requirements. Nonetheless, this initiative shows a constant effort of the European Commission to help companies comply with the GDPR. This creates an atmosphere of transparency and protection when manipulating personal data. In that way, the GDPR is a powerful regulation, and if well enforced, will contribute to AI advances and accuracy thorough a constant trustful relationship between people and companies.

4.4 Policy Options for AI

Drafting effective policies for AI can guide society and prevent future issues. The need for new regulations will increase if the collection and use of digital information are not controlled. The Future of Life Institute addressed fourteen topics in specific areas, which need proper regulations. Most of the suggestions come from Google AI principles, DeepMind, The Information Technology Industry (ITI), Charlevoix Common Vision for the Future of Artificial Intelligence,

[276] European Commission, *Policy Artificial Intelligence*, Digital Single Market, https://ec.europa.eu/digital-single-market/en/artIificial-intelligence (last update Dec. 09.219).

Ethically Aligned Designed (IEE), and Asilomar AI principles. The first principle is enabling AI research and development, which means the right environment to expand beneficial research for AI through a safety program with a high-quality dataset. Second, global governance, race conditions, and international cooperation pointed out key factors, such as collaboration between governments, open dialogue about developments, and advances in discoveries in AI.[277]

The third topic is the economic impact, labor shifts, inequality, and technological unemployment, which focus on the need for retraining programs. The fourth topic is accountability, transparency, and explainability which raises issues around the lack of transparency and explainability linked to machine learning and how to direct liability for misbehavior. The fifth topic is surveillance, privacy, and civil liberties which is an approach related to how companies need to be transparent with privacy policies. [278]

The sixth topic is fairness, ethics, and human rights, concentrating on discrimination, equity, algorithmic bias, and human rights, including the implications of AI on social justice. The seventh topic is political manipulation and computational propaganda, controlling fake news, and how this can be a big challenge. The eighth topic is human dignity, autonomy, and psychological impact, and how AI may control people's lives and make them lose control. The ninth topic addresses human health, argumentation, and brain-computer interfaces by indicating the challenges associated with access to care, control data, and implantation of devices in the human body. The tenth topic states AI safety delimiting mechanisms, control problems, how to prevent accidents, and so on.

[277] Future of Life Institute, *AI Policy Challenges and Recommendations*, https://futureoflife.org/ai-policy-challenges-and-recommendations#Research(last visited Feb.03.2020).

[278] *Id.*

The eleventh topic alleges the security and cybersecurity of how to protect people from powerful AI with many vulnerabilities and calls for the necessity of applying the existent treaty and the creation of new ones. The twelfth topic asserts autonomous weapons and how much autonomy is being given to these systems. The commitment of the big technology companies not to contribute to AI weapons projects is a crucial point. The thirteenth topic is devoted to catastrophic and existential risk, and how AGI can be harmful in the long term, including the combination of AGI and nuclear robotic drones. The last point discusses how AGI can surpass human intelligence.[279] All points raised by the contributors are important for drafting effective policies. For each of these points, the Future Life Institute presents a list of research conducted to embrace these subjects. The figure below shows some of the fields to which AI applies, and how this new technology is part of humans' lives.[280]

[279] Future of Life Institute, *supra note 277.*

[280] *Id.*

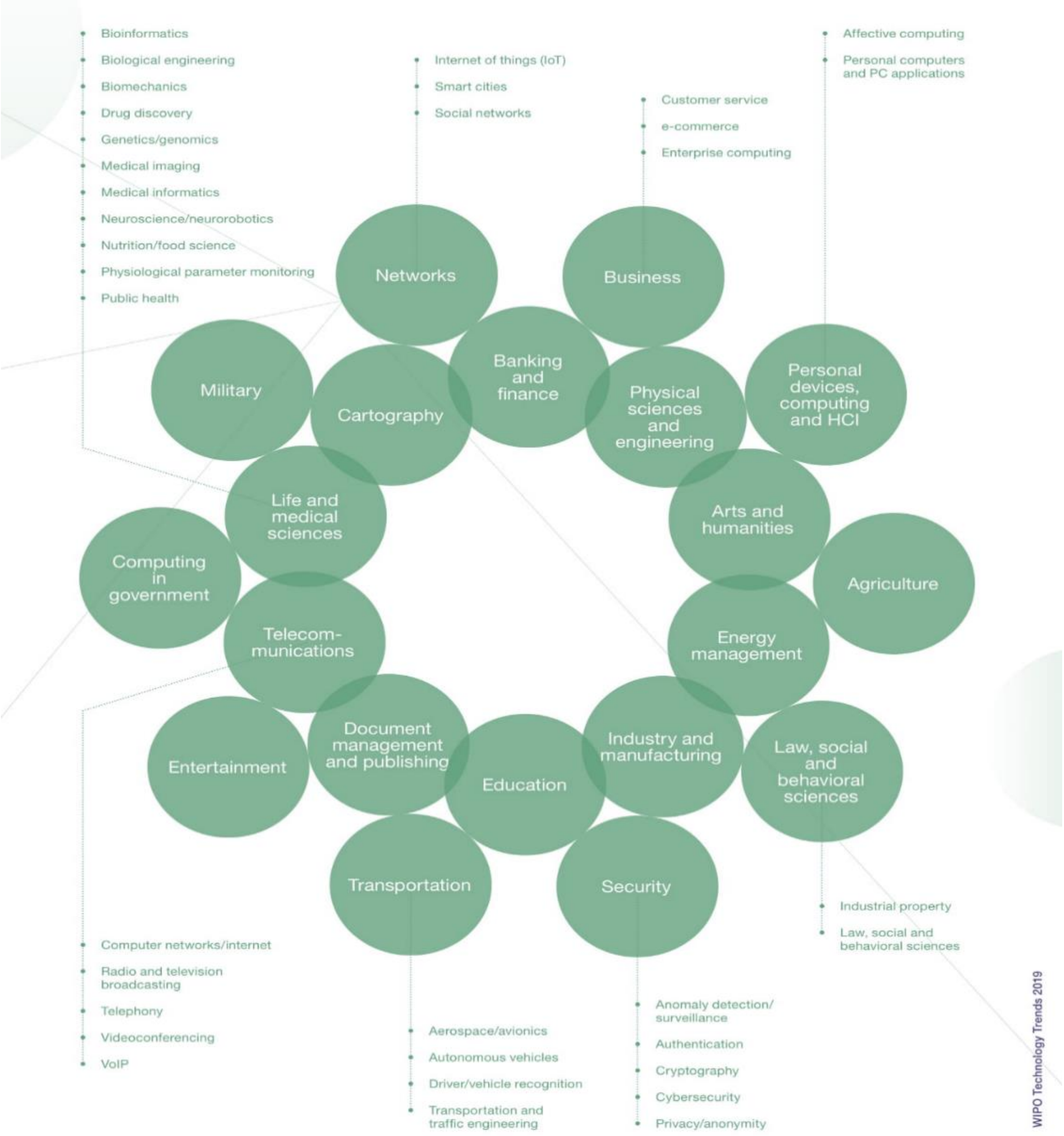


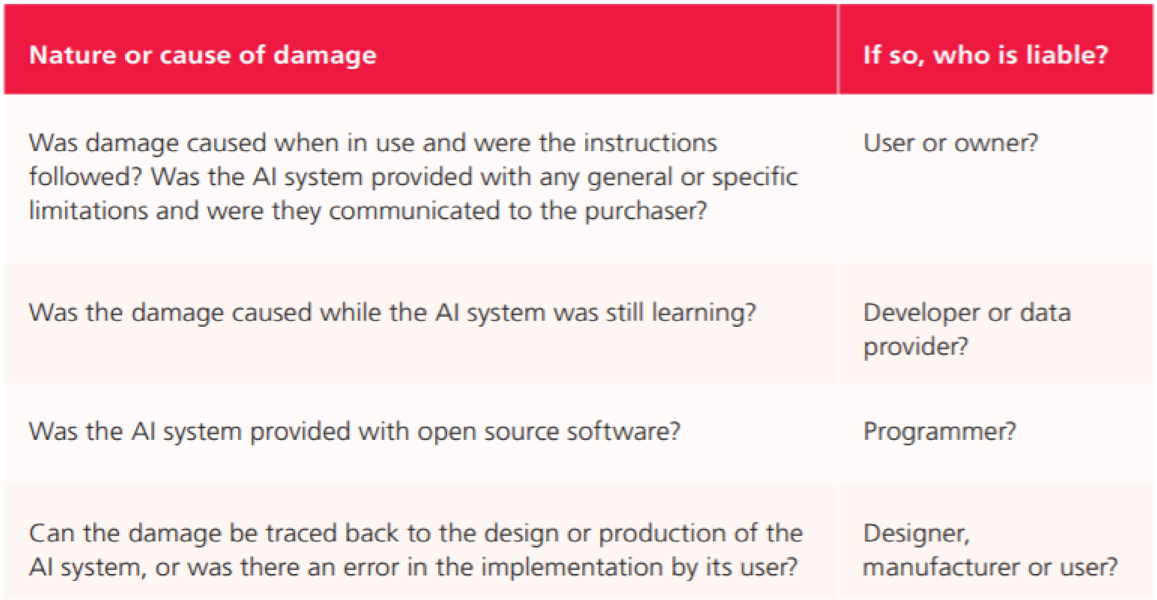
Figure 4. AI applications field.[281]

[281] WIPO *Technology Trends 2019: Artificial Intelligence*. World Intellectual Property Organization (2019). https://www.wipo.int/tech_trends/en/artificial_intelligence/story.html

4.5 Liability in AI.

When AI does not perform well, it can injure, discriminate, or even result in the death of an individual. The first question is who is liable? Who will be sued? Lee Gluyas et al. argue, "A driverless car runs over a pedestrian; a drone partially operated by a pilot crashes and causes damage; an AI software program diagnoses the wrong medical treatment."[282] Thus, to decide who is liable for the harm, it is important to offer some relief or remedy when possible. Below is a chart that illustrates ways to analyze liability.

Table 3
Who Is at Fault When an AI System Fails to Perform?[283]



Nature or cause of damage	If so, who is liable?
Was damage caused when in use and were the instructions followed? Was the AI system provided with any general or specific limitations and were they communicated to the purchaser?	User or owner?
Was the damage caused while the AI system was still learning?	Developer or data provider?
Was the AI system provided with open source software?	Programmer?
Can the damage be traced back to the design or production of the AI system, or was there an error in the implementation by its user?	Designer, manufacturer or user?

[282] Lee Gluyas et al., *Artificial Intelligence- Who is Liable when AI fails to perform?* CMS Law. Tax https://cms.law/en/gbr/publication/artificial-intelligence-who-is-liable-when-ai-fails-to-perform (last visited Feb. 23.2020).
[283] *Id.*

This question and the nature or cause of the damage is what the courts consider in determining liability in many countries with issues related to AI.

4.6 Privacy and Security

With the onset of technology, privacy security becomes almost impractical. As Neil Postman pointed out, "Technology giveth and technology taketh away, and not always in equal measure. A new technology sometimes creates more than it destroys. Sometimes, it destroys more than it creates. But it is never one-sided."[284] The technological advances have brought many conveniences for humans' lives and many headaches. Julie Mehan asserts, "[T]echnology can be a double-edged sword. Reconciling technology, privacy, and security to achieve a workable balance can be a daunting task."[285] The powerful detractors, such as computers viruses and hackers are imperceptible and can be inside a smart phone, a computer, a message from a friend, or many other imaginable ways, so all society is vulnerable.

Some experts assert that society is in an age where a considerable number of crimes have been happening with the capacity to destroy more than a bomb. Cyberwarfare[286] is one of these devastating technologic weapons that can destroy a nation or government's structural organization. Nevertheless, the question is who is committing these crimes and other cyber-attacks? These people are known as hackers. Dorothy Denning asserts,

> The world of computer networking seems to be an anomaly in the firmament of networks. Stories about attacks, breakins, disruptions, theft of information,

[284] Neil Postman, *Technology: Informing Ourselves to Death*, A speech given to Gesellschaft fü Informatik. Stuttgart, Germany (Oct. 1990). https://www.memoriapress.com/articles/informing-ourselves-death/

[285] JULIE MEHAN, CYBER WAR, CYBER TERROR, CYBER CRIME AND CYBER ACTIVISM, ch.1 (2d Ed. 2014) (E-book).

[286] Cyberwarfare: the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.
Dictionary Lexico, cyberwarfare https://www.lexico.com/definition/cyberwarfare (last visited Dec.26, 2019).

> modification of files, and the like appear frequently in the newspapers. A diffuse group called 'hackers' is often the target of scorn and blame for these actions.[287]

Thus, corporations, governments, and people can be the next unlucky victims. Cyber-attacks have been occurring since the advent of the Internet, and the solutions to eradicate these crimes are still a piece of the puzzle.

In this investigation, it has been indicated that a lot of data has been used to achieve different goals in the corporate sector. However, how much of this data has been used for trustful activities? Privacy is facing powerful enemies. To provide safe cyberspace, each day is more challenging for governments and private companies. In the United States, Michael Chertoff, the former Secretary of Homeland Security, during a National Constitution Center debate in 2017, "argued in favor of company cooperation with law enforcement. He said the matter boils down to little more than an obligation to assist whenever possible."[288] According to Chertoff, allowing companies to access all personal information, including texts, videos, audios, and pictures that people exchange, in order to keep the country safe from any harm, is not outrageous.

Throughout history, society has fought for freedom, and with the advent of technology, perhaps this is disappearing. What are the boundaries between privacy and security? It does not seem to make sense to disclose all information if the government cannot assure that it will be in safe hands. Perhaps the problem started in 2013 when Edward Snowden, a former contractor of the National Security Agency (NSA),[289] exposed "U.S. intelligence gathering, cyber practices and

[287] Dorothy E. Denning, *Concerning Hackers Who Brake into Computers Systems*, https://dl.packetstormsecurity.net/docs/hack/denning.html, (last visited Dec.26, 2019).

[288] National Constitutional Center *Privacy vs. Security: Experts Debate Merits of Each in Tech-Rich World* (Jul. 2017), https://www.govtech.com/policy/Privacy-vs-Security-Experts-Debate-Merits-of-Each-in-Tech-Rich-World.html

[289] The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both signals intelligence (SIGINT) and information assurance (now referred to as cybersecurity) products and services, and enables computer network operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.
NSA, Mission and Values, Mission statement https://www.nsa.gov/about/mission-values/ (last visited Dec.26, 2019).

operations many of them at targeted U.S., Internet platforms, and software and hardware providers."[290] After that, technology companies responded to these revelations by enforcing themselves as global actors. Adam Segal states, "Numerous countries have reacted to the Snowden disclosures by promoting industrial policies that avoid U.S. infrastructure, pressing for concessions from American technology companies, forcing companies to store data locally, or supporting domestic competitors.[291] Due to this, "tech officials have argued for a more expansive definition of cybersecurity that focuses on the needs of all users and companies, rather than a more narrow definition centered on U.S. national security."[292] Consumers are apprehensive about the security offered by tech companies, including all personal data shared through smart phones and apps. If personal data is accessed by people with malicious intent, this can be harmful to society in many ways. This risk always exists. Users trust that technology companies are safe when sharing information through apps, but governments are pressing corporations to lower their security protocols to provide better national security.

To understand security better, messages, pictures, and everything else exchanged using the Internet is encrypted.[293] Encryption is a codification that offers protection to the messages that only the receiver can read. For example, two big tech companies, Apple and Google, have a system called "encrypted by default:" "All the data stored on the phone itself will be unreadable to anyone who accesses the phone without knowing the device passcode, in order to unlock the

[290] Adam Segal, Bridging the Cyberspace Gap: Washington and Silicon Valley, 67 INST. NAT'L STRATEGY, NAT'L SEC., no.2, (2017).
[291] *Id.* at 68.
[292] *Id.*
[293] Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptograph.
Margaret Rouse at al. *Definition Encryption* https://searchsecurity.techtarget.com/definition/encryption
(last visited Dec.26, 2019).

encryption."[294] This provides protection for consumers' privacy. However, how do companies manage this powerful protection when the matter is about a crime? Can the government force privates companies to disclose information? Adam Segal states,

> [M]ore than 90 percent of American military and intelligence communications travel over privately owned backbone telecommunications networks. Many of the most talented hackers are in the private sector, and private security firms such as CrowdStrike, FireEye, and Cylance have taken an increasingly large public role in tracing cyberattacks to nation-states and other perpetrators. In addition, Alphabet, Amazon, Apple, Cisco, Facebook, IBM, Intel, and other companies drive innovation and the deployment of new technologies, especially in cutting-edge areas like artificial intelligence.[295]

It appears as though the government is trying to have access to all information people exchange in order to protect society, thereby taking away any privacy; companies are exploiting new technologies and clients' privacy protections. In Brian W. W. Kernighan's words,

> Governments use the word security in the sense of 'national security' that is, protecting the country as a whole against threats like terrorist attacks. Corporations use the word to refer to the protection of their asset from criminals and other companies.[296]

Finding the balance between the differentiation of the security approach seems important for providing the correct protection.

In 2016, a polemic case involving Apple and the Federal Bureau of Investigation (FBI), displayed how some companies have been reacting to the encryption backdoor.[297] In short, the case was about Farook and his wife, Tashfeen Malik, who killed 14 people in December 2015 in San

[294] Center for Democracy & Technology, *Issue Brief: A "Backdoor" to Encryption for Government Surveillance* (Mar. 2016), https://cdt.org/insights/issue-brief-a-backdoor-to-encryption-for-government-surveillance/

[295] Segal, *supra* note 290, at 67.

[296] Brian W. Kernighan, *Understanding the Digital World: What You Need to Know about Computers, the Internet, Privacy, and Security*, 240 (Princeton University Press, 2017).

[297] Encryption backdoor - a backdoor is a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms.
Margaret Rouse, *Backdoor (computing)* https://searchsecurity.techtarget.com/definition/back-door
(last visited Dec.26, 2019).

Bernardino, California.[298] The investigators obtained permission to recapture data from their phones. However, without the password, it was impossible to access the iPhone data. Due to this, the FBI required Apple to disclose the information. The corporation negated the access, contending that the government was using the case to have more power over anyone's device.[299] It is an extremely sensitive area of discussion, particularly when considering that security and privacy need to work together. Security and privacy are complementary subjects since the act of disclosing data can put people's lives in danger. The question is whether backdoors, and the ability to allow the government to access iPhone encrypted data, is the solution for stopping terrorism or cyberattacks. This complex question is what governments are trying to solve through regulations. David E. Pozen argues that "privacy is constantly being juxtaposed with competing goods interests, balanced against disparate needs and demands."[300] In most situations that deal with privacy, problems will prevail in the public interest and sometimes the private interest. There is no inaccurate side, but the situation is getting worse and the dialogue between governments and private companies is fundamental to keeping privacy and security on the same page. Moreover, some trade-offs are required. Governments can create safe data flows to companies, and in exchange, corporations need to inform governments about how the data is used and promise that they will not use data for different purposes without authorization. This generates a balanced relationship between privacy, society, government, and business.

[298] John Mueller, CASE 76: SAN BERNARDINO https://politicalscience.osu.edu/faculty/jmueller/76SANB7.pdf

[299] Evan Perez and Time Hume, *Apple opposes judge's order to hack San Bernardino shooter's iPhone, CNN* (Feb. 2016), https://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html

[300] David E. Pozen, *Privacy-Privacy Tradeoffs*, 83, 222 U. Chi. L. Rev. no 1(Winter 2016).

4.7 The Legal Requirements for Automated Decision-Making

Machines have some vulnerabilities and these can lead to mistakes, such as the prescription of a wrong medicine to a patient, denial of a loan for a student, and so on. The following question remains: When machines make inaccurate decisions about humans, will the court judge and provide a remedy? When machines cause damage, what are the legal requirements? Chris M. Temple argues,

> If the smart process system was not defective and performed as intended, but an injury causing decision occurred, can we recreate the circumstances and the machine's reasoning process and judgment as a technical matter or in a manner suitable for evidentiary requirements in a subsequent court proceeding? In other words, can the assembled system of interconnected equipment 'testify' based on stored data? If the data becomes unavailable, questions will arise whether evidence is being destroyed.[301]

There are more questions than answers for decision-making. The author raises the issue of when there is no record of a machine's decision, and how one proves a mistake if it is not traceable. Perhaps, laws should require corporations to keep all data used in decision-making. One way to ensure transparency in the corporate decision-making process is to impose liability on corporations when they cannot provide or prove a record of data used. However, there is also a need for corporations to take data usage into consideration besides complying with privacy laws.

4.8 Blockchain and AI

Authors are using the "fourth industrial revolution" terminology to describe all changes and advances that AI will bring. Blockchain and AI seem to be a powerful combination. Before

[301] Chris M. Temple, *AI-Driven Decision-Making May Expose Organizations to Significant Liability Risk*, Corporate Compliance Insights (Sept. 11.2019), https://www.corporatecomplianceinsights.com/ai-liability-risk/

proceeding, it is necessary to explain the blockchain technology. Vinay Trivedi asserts, “Blockchain technology sometimes referred to as distributed ledger technology, is one of the latest innovations in technology. It has applications in a whole host of fields including finance, law, economics, mathematics, philosophy, and computer science.”[302] The author states that blockchain is a different way to store data. Blockchain has an advantage over other forms of saving data because it contains important elements, such as transparency, trust, and verifiability, which is suitable for AI. One of the benefits of blockchain to AI is the possibility to share machine-learning models between parties without an intermediary.[303] To synthesize, AI systems need a set of data to execute different purposes, and the more data that can be accessed, the more accurate AI is.

Akash Takyar expounds,

> [M]ost AI-based projects need to store data on centralized servers or the cloud. In such cases, there is a single-point-access to the data, which is more vulnerable to security attacks. Being a decentralized system, Blockchain provides the ideal solution to centralized data storage. It allows AI-based systems to store their data on multiple systems spread across the globe and at the same time, access them seamlessly. It also enables access to a much-diverse data set, facilitating better and more profound learning of AI/ML algorithms.[304]

Blockchain seems to be the perfect marriage with AI since most of the concerns about machine learning are around how to keep data safe, especially sensitive data. The author specifies that in industries such as healthcare and finance that deal with sensitive data, Blockchain is crucial to ensuring complete protection of data through cryptographic encryption. Hence, through technological protections such as Blockchain, AI developers can build a trustful relationship between consumers, governments, and society.

[302] VINAY TRIVEDI, HOW TO SPEAK TECH: THE NON-TECHIE’S GUIDE TECHNOLOGY CONCEPTS, ch.14 (Apress, 2019) (eBook).

[303] Ron Schmelzer, *AI and Blockchain: Double the Hype or Double the Value?*, Forbes (Oct. 24.2019), https://bit.ly/2HQoIPV

[304] Akash Takyar, *Blockchain and AI- Towards the “Forth Industrial Revolution”*, LeewayHertz, https://www.leewayhertz.com/blockchain-and-ai/ (last visited Feb.24.2020).

4.9 Regulations and Limitations to Data-Transfers

With the Internet of things providing so many possibilities for business, there is a constant need to protect different transactions. Through one click, a person is able to buy perfume even though the factory is located in Paris, but the buyer is in California sitting in front of a computer. It does not matter where the buyer or company is located; the product can be sent anywhere. The question here is how to protect trans-border data-transfers in a world without borders for e-commerce.[305]

According to the United Nations Conference on Trade and Development (UNCTAD),

> Data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices. The relationship between data protection and information and communication technologies ICT developments changes all the time, - but can be demonstrated by three recent developments. 1. Cloud computing 2. The Internet of Things 3. Big Data analytics Each of these technologies presents new challenges to data protection, particularly in the areas of the definition of 'personal data' and the management of cross-border data transfers.[306]

Hence, the transfer of data between countries is also a subject of data protection law. The GDPR does not limit the transfer of data between its members or across borders. As Qi Zhu affirms, "Any EU Corporation that has set up branches in China and processes EU personal data or any Chinese corporation that has set up branches in the EU and processes EU personal data, must check their compliance with the GDPR in a timely manner, thereby avoiding business compliance risks."[307]

[305] See Ecommerce guide, what is ecommerce? https://ecommerceguide.com/guides/what-is-ecommerce/ (last visited Feb.24.2020).

[306] United Nations Conference on Trade and Development UNCTDA, *Data protection regulations and international data flows: Implications for trade and development*, 10 (2016), https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

[307] Qi Zhu, *Data Research: Compliance with Cross-Border Personal Data Transfer Limitations, Lexology* (Jun.25, 2019), https://www.lexology.com/library/detail.aspx?g=7dff1512-40ab-4614-a3fe-f435a5b7a37f.

Therefore, Chinese corporations or other companies around the world need to comply with the transfer of personal data to third countries or international organizations of the GDPR, as outlined in Chapter 5.[308] Nonetheless, Qi Zhu, alleges that

> [F]or foreign corporations in China and local Chinese corporations, the processing of Chinese citizens' personal data is restricted not only by extraterritorial regulations such as the GDPR, but also by local Chinese data protection laws. Under the current legislation in China, legal regulation of cross-border personal data transfer is a key point for data protection.[309]

However, China does not have guidelines for the specific requirements, including how companies need to comply with the law in terms of data localization and security assessment related to cross-border data transfer.[310]

Working together, the EU, the U.S. Frameworks from the U.S. Department of Commerce, the European Commission, and the Swiss Administration designed a framework for privacy shield to provide companies with a compliance mechanism for commerce among them. Guiding the three legal systems involved in the shield, the framework explains how to comply with data protection provisions when transferring personal data between the EU, U.S., and Switzerland.[311] Thereby, cross-bother personal data transfer is also in a period of adaptation, and corporations are trying to comply with laws and requirements. Some companies are implanting internal policies according to the strictest requirements to create a standard and then operate those in internal and foreign markets without issues.

[308] REGULATION (EU) (GDPR) 2016/679, 2016 O.J. (L 119/60-62).

[309] Qi Zhu, *Data Research: Compliance with Cross-Border Personal Data Transfer Limitations, Lexology* (Jun.25, 2019), https://www.lexology.com/library/detail.aspx?g=7dff1512-40ab-4614-a3fe-f435a5b7a37f.

[310] Hongquan (Samuel) Yang, *The Privacy, Data Protection and Cybersecurity Law Review: Overview*, (Oct.2019), https://bit.ly/2wtB0Lv

[311] Privacy Shield Framework, *Privacy Shield Program Overview*, https://www.privacyshield.gov/Program-Overview (last visited Feb.24.2020).

Besides the framework of data protection in the three legal systems and related rules of transfer of data, the Organization for Economic Co-operation and Development (OECD)[312] launched guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. These guidelines were revised in 2013. They offer advice to the public and private sectors on the manners with which personal data are processed. The guidelines apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, its nature and context they are used, that poses a danger to privacy and individual liberties."[313] In the revised version, the OECD addresses seven points, taking into consideration how the collection of data underwent a deep change in the economy and daily life, and how societies have changed in the last 30 years since the first guidelines were written. While the first point addresses the volume of data collected and stored, the second deals with the range of analytics and how the data started to be used. The third point is the value of responsible use of personal data, delivering benefits to society. The fourth is the extension of threats related to privacy. The fifth point is the number and variety of actors that put the protection of privacy and others at risk. The sixth focuses on the frequency and complexity of interactions involving personal data and how individuals can understand and negotiate it. The seventh and last point addresses the global availability of personal data. Thus, the guidelines assist countries to understand the importance of privacy as a fundamental right and how to deal with technology versus the privacy of individuals.[314] It is crucial in the digital age that governments study ways to achieve the appropriate balance between privacy and technology and provide the appropriate protection for personal information.

[312] OECD, *Wo we are,* https://www.oecd.org/about/, (last visited Mar.21.2020).
[313] Organization for Economic Co-operation and Development (OECD), *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and TransBorder Flows of Personal Data*, C(80)58/FINAL (Sept. 23, 1980).
[314] OECD, The OECD Privacy Framework (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

CHAPTER 5: FINAL CONSIDERATIONS

The objective of this thesis was to investigate how data protection works in the context of AI and its legal implications. First, the research shows the inadequacy of existing law to address the appropriate and effective protection of privacy and data in the age of AI. National legislation on privacy and data protection is not necessarily equipped to address the impact of AI on the protection of data and privacy. While the law specifically addresses the implications of AI, it is still inadequate because the law is often unable to keep up with the speed of technological advancements. This means that technological advances are ahead of laws. Second, it is a fact that privacy issues have always existed, and in the digital era with AI innovations, privacy challenges have become more frequent. Personal information is more readily available; through tools, such as search engines, social media, cellphones, and the advent of e-commerce, personal data is being gathered and exploited. Nevertheless, the protection of privacy as a fundamental right remains the same. The use of data for different purposes seems to be crucial to AI developments. On the other hand, AI developments cannot surpass the expectation of the "right to be let alone" and the "right to be forgotten," which requires specific laws that address privacy and AI needs. Third, it is undeniable how many benefits AI brings to different areas of expertise by also changing the way people work, act, react, and think. It appears that laws that create barriers to AI are not the solution since the assets it provides do not have boundaries. The crucial point is transparency in the process—that is, to consumers as owners of personal data with control over how their data will be used. Consumers have the right to practice their fundamental right to say no to projects they do not agree with, especially if they are not sure about the company's purposes.

This thesis focused on the three legal systems of the EU, China, and the U.S.. It was found that the concept of privacy varies among the three systems, which perhaps make them provide different protections to privacy. The EU, with the concept of privacy as a fundamental right guaranteed in the GDPR, provides what was considered up to this point one of the most robust regulations related to the processing of data. Nonetheless, the flow of data to AI developments seems fundamental, which is making the EU rethink new ways to approach and solve the friction between AI and GDPR. On the other hand, China has different concepts of liberty and privacy than those of western countries, and adopted the CSL with a different focus. The CSL keeps the monopoly of data in China, creates a barrier for foreign companies, providing growth for national companies, and at the same time, controlling the privacy of Chinese citizens through government interest. The U.S. regulates privacy through a set of federal and state laws. However, the state of California with the enacted CCPA shows a strong tendency to have strong regulations on privacy that include businesses manipulating personal data.

Given the findings of this investigation, the following suggestions seem pertinent to the field. The technological advent exposed how vulnerable society is and how it is unprepared to face the changes that AI tools bring. It is crucial to have robust laws to drive society to general welfare—that is, elaborate laws focused on humanity and prosperity. It is time to embrace rules that are strong enough to prevent a general collapse. Rules that can protect the right to be let alone as a fundamental right protected in constitutions around the world. Yes, machines can learn, and in the near future, they are going to lead functions that were previously led by humans. There is no way to stop reality. However, machines are human creations, and thus, they rely on human input. This dependent relationship means the outcomes of machines can be forecasted and driven by humans. The present generation is facing issues linked to privacy, liability, and safety. There are ways to prevent these issues and find a balance between privacy, technology, and protection. The development of AI is fully integrated with the data humans generate, and this means the processes of collecting data need to be regulated in order to protect privacy. Thus, regulated processes need to be traceable to discover how decisions are made, and if these decisions match reality. Laws need to determine how much time a machine needs to be trained and controlled before an operation and who will be responsible for undesirable or unsatisfactory outcomes. The urgency of broad regulations to ensure responsibility in the innovation process is crucial because AI has affected individuals' privacy.

Moreover, society must take into consideration how the Internet drove society to a world without borders. Given the importance of the topic to humanity and the global nature of the problem, an international regulation following the EU model and some of the OECD guidelines might provide some guidance. Regulation at the international level would prepare humanity for better protection of the flow of data and information on a global scale. The achievement of this research was discovering the roots and nature of privacy and the primordial importance of keeping personal information safe. It provided an opportunity to navigate the technological AI universe and discover that AI is involved in almost every single program used today. The new ways of interacting with technology have changed the ways humans buy, see, express feelings, and communicate. However, these transformations cannot reverse the fact that privacy is a fundamental right and needs to be respected at all levels of innovation. Thus, the harmonization between privacy and AI is paramount for more astonishing breakthroughs.

BIBLIOGRAPHY

Act, F. T. (n.d.). *Federal Trade Commission Act*. Retrieved from https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act

Alexa, A. (2020, FEB. 21). *Alexa Science: Delivering Tomorrow's Vision for Conversational AI Today,* . Retrieved from AMAZON: https://developer.amazon.com/pt-BR/alexa/science

Ames, M. G. (2020, Jan 15). *The Evil list which tech companies are really doing the most harm? Here are the 30 most dangerous, ranked by the people who know, Slate, technology*. Retrieved from Slate Technology: https://slate.com/technology/2020/01/evil-list-tech-companies-dangerous-amazon-facebook-google-palantir.html

Anglim, C., Nobahar, G., and Kirtley, J. E. (2015). *Privacy Rights In The Digital Age.* Grey House Publishing.

Apple. (2020, Apr. 9). *Use Siri on all your Apple devices*. Retrieved from Apple: https://support.apple.com/en-us/HT204389

Arruda, A. (2017, Nov. 6). *Defining Artificial Intelligence with AI pioneers Bengio, Hinton, Ovbiagele & P M Tradeau*. Retrieved from ROSS: https://blog.rossintelligence.com/post/ai-pioneers-bengio-hinton-ovbiagele-pm-trudeau

Bank of American (2018, Oct 22). *Introducing Erica Insights: Bank of America's AI- Driven Virtual Financial Assistant Just Got Smarter*. Retrieved from Bank of America : https://newsroom.bankofamerica.com/press-releases/consumer-banking/introducing-ericar-insights-bank-americas-ai-driven-virtual

Becerra, X. (2020, Feb 11). *California Consumer Privacy Act (CCPA), Modifications to proposed Regulations – released February 10, 2020 15 day Comment Period- ended February 25, 2020*. Retrieved from State of California Department of Justice: https://oag.ca.gov/privacy/ccpa

Becerra, X. (2020, March 27). *California Consumer Privacy Act (CCPA), Modifications to proposed Regulations – released March 11, 2020 Deadline to Submit written Comments: March 27, 2020 at 5 pm*. Retrieved from State of California Department of Justice: https://oag.ca.gov/privacy/ccpa

Binns, R. (2019, Jul. 25). *Information Commissioner's Office, iCO., Trade-offs*. Retrieved from WIREDGOV: https://www.wired-gov.net/wg/news.nsf/articles/Tradeoffs+25072019151000?open

Bolter, J. D. (1984). Artificial Intelligence, Vol.113, No.3. *Daedalus*, 1-18.

Bond, S. (2019, Nov. 25). *Defining Data intelligence : Intelligence about Data, Not from Data*. Retrieved from IDC: https://blogs.idc.com/2019/11/25/defining-data-intelligence-intelligence-about-data-not-from-data/

Bukaty, P. (2019). *California Consumer Privacy Act (Ccpa): An Implementation Guide.* ITGP.

Bunz, M. A. (2018). *Artificial Intelligence And The Internet Of Things Uk Policy Opportunities And Challenges.* University of Westminster Press.

Business, F. (2018, Jan. 29). *Facebook's commitment to data protection and privacy in compliance with the GDPR*. Retrieved from Facebook Business: https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr

Calder, A. (2013). *The Case for ISO27001:2013, 51* . It government Publishing.

Californians for Consumer Privacy (2020, Jan 25). *What goals does the California Consumer Privacy Act accomplish?* Retrieved from Californians for Consumer Privacy: https://www.caprivacy.org/faq/

Carson, A. (2020, Apr. 14). *Critics say attorney general's proposed CCPA regulations add confusion, not clarity*. Retrieved from iapp: https://iapp.org/news/a/critics-say-ags-proposed-ccpa-regulations-add-confusion-not-clarity/

Castro, D. and Chivot, E. (2020, Mar. 23). *Want Europe to have the best AI? Reform the GDPR*. Retrieved from iapp: https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/

Cate, F. H., Dockery, R. (2019). *Artificial Intelligence and Data Protection: Observations on a Growing Conflict*. Retrieved from Ostrom Workshop: https://ostromworkshop.indiana.edu/pdf/seriespapers/2019spr-colloq/cate-paper.pdf

Center for Democracy & Technology (2016, Mar 3). *Issue Brief: A "Backdoor" to Encryption for Government Surveillance*. Retrieved from Center for Democracy & Technology: https://cdt.org/insights/issue-brief-a-backdoor-to-encryption-for-government-surveillance/

Center for Disease Control and Prevention (2018, Sep. 14). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Retrieved from Center for Disease Control and Prevention: https://www.cdc.gov/phlp/publications/topic/hipaa.html

CCPIT Patent & Trademark Law Office. (2019, Apr. 26). *The Revised PRC Anti-Unfair Competition Law Took Effect on April 23, 2019*. Retrieved from CCPIT Patent & Trademark Law Office: https://www.ccpit-patent.com.cn/node/6183

Chang, A. (2018, May 02). *The Facebook and Cambridge Analytica Scandal, explain with a simple diagram*. Retrieved from Vox: https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Cheatham, B., Javanmardian, K. and Samandari, H. (2019, Apr). *Confronting the risks of artificial intelligence.* Retrieved from McKinsey Quarterly: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence

Chen, J. (2019, Jul. 5). *What was the Insdustrial Revolution* Retrieved from Investopedia : https://www.investopedia.com/terms/i/industrial-revolution.asp

Cherry, D. (2013). *The Basics of Digital Privacy.* Syngress.

China SME IPR. (2010). *Copyright Protection in China.* Retrieved from https://www.china-iprhelpdesk.eu/: https://www.china-iprhelpdesk.eu/sites/all/docs/publications/EN_Copyright_guide_Aug_2010.pdf

Christakis, S. (2019, Jul.). *Data Privacy is the New Strategic Priority*. Retrieved from IBM: file:///C:/Users/Ana%20Paula/Downloads/IBM_WP_2019_Data%20Privacy%20Is%20The%20New%20Strategic%20Priority.pdf

Clement, J. (2020, Apr 30). *Facebook: Number of monthly active users worldwide 2008-2020.* Retrieved from Statista : https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Commission, E. (2019, Dec. 09). *Policy Artificial Intelligence, Digital Single Market*. Retrieved from European Commission.

Commission, E. (2020, Feb. 19). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data*. Retrieved from European Commission: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

Cook, D. J., and Krishnan, N. C. (2015). *Activity learning : discovering, recognizing, and predicting human behavior from sensor data.* Hoboken, New Jersey : John Wiley & Sons , Inc.

Cooke, J. W. (1973). Jefferson on Liberty, Vol. 34, No. 4 . *Journal of the History of Ideas*, 563-576.

Cosgrove, C. (2020, Mar 17). *Analyzing the second set of modifications to draft CCPA regulations*. Retrieved from iapp: https://iapp.org/news/a/analyzing-the-second-set-of-modifications-to-draft-ccpa-regulations/

Cosgrove, C. (2020, Mar 17). *Analyzing the second set of modifications to draft CCPA regulations*. Retrieved from iapp: https://iapp.org/news/a/analyzing-the-second-set-of-modifications-to-draft-ccpa-regulations/

Davidow, W., and Malone, M. S. (2020). *The Autonomous Revolution: Reclaiming the Future We've Sold to Machines.* Berrett-Koehler Publishers.

Day one Staff (2018, Jul. 09). *Amazon AI Protecting data privacy: How Amazon is advancing privacy-aware data processing*. Retrieved from Amazon: https://blog.aboutamazon.com/amazon-ai/protecting-data-privacy

De Guise, P. (2017). *Data Protection : Ensuring Data Availability.* Auerbach Publishers, Incorporated.

Denning, D. E. (n.d.). *Concerning Hackers Who Brake into Computers Systems*. Retrieved from https://dl.packetstormsecurity.net/docs/hack/denning.html

Dictionary, C. (n.d.). *Data*. Retrieved from Dictionary, Cambridge: https://dictionary.cambridge.org/dictionary/english

Ecommerce Guide. (n.d.). *what is ecommerce?* Retrieved from Ecommerce guide: https://ecommerceguide.com/guides/what-is-ecommerce/

Eidam, E. (2017, Jun. 7). *National Constitutional Center Privacy vs. Security: Experts Debate Merits of Each in Tech-Rich World.* Retrieved from Gt Government Technology: https://www.govtech.com/policy/Privacy-vs-Security-Experts-Debate-Merits-of-Each-in-Tech-Rich-World.html

Epic.org. (n.d.). *The right to be forgotten (Google v. Spain)*. Retrieved from epic.org: epic.org, https://epic.org/privacy/right-to-be-forgotten/

Etzioni., A., and Etzioni, O. (2017). Should Artificial Intelligence Be Regulated? *Issues in Science and Technology*, 32-36.

European Union (n.d.). *General presentation*. Retrieved from Court of Justice of the European Union: https://curia.europa.eu/jcms/jcms/Jo2_6999/en/

European Data Protection Supervisor (n.d.). *The EU'S independent data protection authority, Data Protection*. Retrieved from European Data Protection Supervisor: https://edps.europa.eu/data-protection/data-protection_en

European Data Protection Supervisor (n.d.). *The History of the General Data Protection Regulation*. Retrieved from European Data Protection Supervisor: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

European Patent Office. (2019, Oct 01). *Guidelines for Examination.* Retrieved from https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm

European Union (2019, Mar 13). *Single Market, A single internal market without borders*. Retrieved from European Union: https://europa.eu/european-union/topics/single-market_en

Evans, W. (2019, Dec. 5). *Ruthless Quotas at Amazon Are Maiming Employees his holiday season, Amazon will move millions of packages at dizzying speed. Internal injury reports suggest all that convenience is coming at the expense of worker safety*. Retrieved from The Atlantic : https://www.theatlantic.com/technology/archive/2019/11/amazon-warehouse-reports-show-worker-injuries/602530/

Exploring Constitutional Conflicts. (n.d.). *The Right of Privacy: The Issue: Does the Constitution protect the right of privacy? If so, what aspects of privacy receive protection?* Retrieved from Exploring Constitutional Conflicts: http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

Facebook. (n.d.). *We are committed to honoring your privacy choices and protecting your information*. Retrieved from Facebook: https://about.fb.com/actions/protecting-privacy-and-security/

Facebook. (n.d.). *Facebook Brand Resource Center*. Retrieved from Facebook: https://en.facebookbrand.com/

Federal Register the Daily Journal of United State. (2020, Jan 13). *Request for Comments on a Draft Memorandum to the Heads of Executive Departments and Agencies, "Guidance for Regulation of Artificial Intelligence Applications"*. Retrieved from Federal Register the Daily Journal of United States Government: https://www.federalregister.gov/documents/2020/01/13/2020-00261/request-for-comments-on-a-draft-memorandum-to-the-heads-of-executive-departments-and-agencies

Federal Trade Commission Protecting American's Con. (n.d.). *Gramm-Leach-Bliley Act*. Retrieved from Federal Trade Commission Protecting American's Consumers: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Feuerhake, J. (n.d.). *AI, data protection and data ownership*. Retrieved from TaylorWessing: https://iot.taylorwessing.com/ai-data-protection-and-data-ownership/

Fischetti, T. (2018). *Data Analysis with R - Second Edition.* Packt Publishing.

Foundation, O. K. (2009). *Open Data Handbook*. Retrieved from Open Knowledge Foundation: http://opendatahandbook.org/guide/en/what-is-open-data/

Foundation, O. k. (n.d.). *About.* Retrieved from Open Knowledge Foundation: https://okfn.org/about/

Framework, P. S. (n.d.). *Privacy Shield Program Overview*. Retrieved from Privacy Shield Framework: https://www.privacyshield.gov/Program-Overview

Franke, U. (2019). Harnessing Artificial Intelligence. *European Council on Foreign Relations,*

Frontero. (2018, Jul. 30). *Corporate Counsel's New Big Risk Factor: International Privacy Law and Compliance with U.S. Discovery and Investigation Requests*. Retrieved from Frontero Resources Blog: https://www.fronteousa.com/usa/corporate-counsels-new-big-risk-factor-international-privacy-law-and-compliance-with-u-s-discovery-and-investigation-requests/

Future of Life Institute. (n.d.). *AI Policy Challenges and Recommendations*. Retrieved from Future of Life Institute: https://futureoflife.org/ai-policy-challenges-and-recommendations#Research

Future of Life Institute. (n.d.). *Autonomous Weapons: An Open Letter From AI & Robotic Researchers*. Retrieved from Future of Life Institute: https://futureoflife.org/open-letter-autonomous-weapons/

Gibbs, S. (2017, Aug. 20). *Elon Musk leads 116 experts calling for outright ban of killer robots*. Retrieved from The Guardian: https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war

Gimmingsrud, K. (2019, Aug. 20). *Artificial Intelligence and Data Privacy.* Retrieved from Expert Guides: https://www.expertguides.com/articles/artificial-intelligence-and-data-privacy/aruywukr

Gluyas, L., and Day, S. (2018). *Artificial Intelligence- Who is Liable when AI fails to perform?* Retrieved from CMS Law. Tax: https://cms.law/en/gbr/publication/artificial-intelligence-who-is-liable-when-ai-fails-to-perform

Goode, L., Matsakis, L.(2020, Jan. 07). *Amazon Doubles Down on Ring Partnerships with Law Enforcement the Company's top Hardware executive told Wired he's "proud" of the* *controversial program and hinted at a future with more facial recognition.* Retrieved from Wired: https://www.wired.com/story/ces-2020-amazon-defends-ring-police-partnerships/

Gloogle, AI. (n.d.). *Responsible AI Practices, Google*. Retrieved from Google AI: https://ai.google/responsibilities/responsible-ai-practices/?category=privacy,

Grothaus., M. (2018, Dec. 13). *How our data got hacked, scandalized, and abused in 2018*. Retrieved from fastcompany: https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018

Gurry, F. (ed.). (2019). *WIPO Technology Trends 2019 Artificial Intelligence.* WIPO. Retrieved from World Intellectual Property Organization: https://www.wipo.int/tech_trends/en/artificial_intelligence/story.html

Hall, P., Gill, N. (2019). *An Introduction to Machine Learning Interpretability, 2nd Edition.* O'Reilly Media, Inc.

Habber, M. J. and Hibbert, B. (2017). *Organizations, Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect.* Apress.

Hargrave, S. J., and Karnoupakis, E. (2020). *Blockchain Success Stories.* O'Reilly Media, Inc.

Harris, R. (2019, Sept. 01). *Elon Musk: Humanity Is a Kind of 'Biological Boot Loader'for AI*. Retrieved from Wired : https://www.wired.com/story/elon-musk-humanity-biological-boot-loader-ai/

Hemphill, T. A. (2019, Aug. 15). *Artificial Intelligence and the Antitrust Challenges, Inside sources*. Retrieved from Inside sources: https://www.insidesources.com/artificial-intelligence-and-the-antitrust-challenges/

Hildenbrand, J. (2018, Jan 12). *Does Google sell your personal Data? The short answer: no. It's valuable to them if they keep it for themselves*. Retrieved from androidcentral: https://www.androidcentral.com/does-google-sell-your-data

Hoffman, D., Masucci, R. (2018, October 22). *Intel's Ai Privacy Policy White Paper Protecting Individuals 'Privacy And Data In The Artificial Intelligence World.* Retrieved from Intel: https://blogs.intel.com/policy/files/2018/10/Intels-AI-Privacy-Policy-White-Paper-2018.pdf

Holvast, J. (2007). History of Privacy, Holvast & Partner, Privacy Consultants. *NL- Landsmeer, The Netherland*, 13-42.

Hristov, K. (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA: The IP L. Rev.*, 1-24.

Iafrate, F. (2018). *Artificial Intelligence And Big Data: The Birth Of A New Intelligence.* Iste.

ICO, T. I. (n.d.). *who-we-are*. Retrieved from ICO.: https://ico.org.uk/about-the-ico/who-we-are/

IDC, A. t. (2017). *Taxonomy, IDC'S Worldwide Semiannual Internet of Things Spending Guide Taxonomy*. IDC. Retrieved from https://www.ibm.com/downloads/cas/56ZMODLB

Ikeda, S. (2020, Jan 06). *Facebook refuses to Change Web Tracking Practices, Believes That CCPA Does Not Apply to Them*. Retrieved from CPO Magazine: https://www.cpomagazine.com/data-protection/facebook-refuses-to-change-web-tracking-practices-believes-that-ccpa-does-not-apply-to-them/?__cf_chl_jschl_tk__=cd5ec61e913c0d5e7c0532fe5073a005eacd32a2-1582613379-0-AQn5rNmJ7hkRBZno1VcUkQJMMyC7Kl26oQLoyx3UzObL

Insights, S. (n.d.). *Why is Big data important?* Retrieved from SAS Insights: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html

Insights, S. I. (n.d.). *Artificial Intelligence What it is and why it matters*. Retrieved from SAS: https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html#close

Insights, T. (2019, Mar. 27). *Rethink Privacy For the AI Era*. Retrieved from Forbes: https://www.forbes.com/sites/insights-intelai/2019/03/27/rethinking-privacy-for-the-ai-era/#5939ae907f0a

IT Governance Privacy Team (2019). *EU General Data Protection Regulation (GDPR), An Implementation And Compliance Guide.* IT Governance Publishing.

Kakavoulis, K. (2018, Jun. 20). *The Case Google Spain v AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A brief critical analysis.* Retrieved from Homo Digitalis: https://www.homodigitalis.gr/en/posts/2900

Kanclirz, J. (2008). *Netcat Power Tools.* Syngress.

Kernighan, B. W. (2017). *Understanding The Digital World: What You Need To Know About Computers, The Internet, Privacy, And Security.* Princeton University Press.

Kissell, J. (2019). *Take Control of Your Online Privacy, 4th Edition.* Take Control Books.

Koespse, K. M. (2018). *Trade Secrets: A Legal Research Guide, Introduction.* Packt Publishing.

Kushmaro, P. (2018, Sept 27). *5 ways industrial AI is revolutionizing manufacturing, In no other sector, is artificial Intelligence having more of an impact than on manufacturing, and the revolution is just beginning,* Retrieved from CIO: https://www.cio.com/article/3309058/5-ways-industrial-ai-is-revolutionizing-manufacturing.html

Lallement, R. (2017). *Intellectual Property And Innovation Protection.* Wiley-ISTE.

Lau, T. (. (2019, May 23). *When AI Becomes a Part of Our Daily Lives*. Retrieved from Harvard Business Review Home: https://hbr.org/2019/05/when-ai-becomes-a-part-of-our-daily-lives

Leaffer, M. A. (2019). *Understanding Copyright Law.* Carolina Academic Press.

Lee, K.-F. (2018). *Ai Super Powers China, Silicon Valley And The New World Order.* Houghton Mifflin Harcourt Bos. N.Y.C.

Levy, S. (2010). *Hackers heroes of the computer revolution.* O'Reilly Media, Inc.

Lexico, D. (n.d.). *cyberwarfare*. Retrieved from Dictionary Lexico: https://www.lexico.com/definition/cyberwarfare

Li, N., Lyu, M., and Su, D. (2016). *Differential Privacy From theory to Practice (Synthesis Lectures on Information Security, Privacy, & Trust).* Morgan & Claypool.

Liu, H. (2014). *Face Detection And Recognition On Mobile Devices, Morgan Kaufmann* .

Luo, Y., Yu, Z., Fein, A., and Daugherty, M. (2019, Jun. 18). *Cyber Trends in China*. Retrieved from Lexology: https://www.lexology.com/library/detail.aspx?g=2352790f-4414-484d-814e-6c435d3e1956

M.Cooley, T. (1932). *A Treatise On The Law Of Torts: Or The Wrongs Which Arise Independently Of Contract.* Callaghan.

Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., Ko, R., Sanghvi, S. (2017, Nov.). *Jobs Lost, Jobs Gained, Workforce Transitions in a time of Automation*. Retrieved from Mckinsey Global Institute: https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

Marr, B. (2015). *Big Data: Using Smart Big Data, Analytics And Metrics To Make Better Decisions And Improve Performance.* Wiley.

Marr, B. (2016). *Big Data in Practice : How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results.* John Wiley & Sons, Incorporated.

Marr, B., and Ward, M. (2019). *Artificial Intelligence In Practice : How 50 Successful Companies Used Ai And Machine Learning To Solve Problem.* Wiley.

Maule, D. Niu, Z. (2010). *Media Law Essentials.* Edinburgh University Press.

McCarthy, J. (n.d.). *What is AI? / Basic questions what is AI? / Basic questions*. Retrieved from stanford: http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html

McClealland, C. (2020, Jan 15). *The Impact of Artificial Intelligence- Widespread Job Losses*. Retrieved from iot for all : https://www.iotforall.com/impact-of-artificial-intelligence-job-losses/

McJohn, S. M. (2019). *Examples & Explanations Intellectual Property.* Walters Kluwer.

McKay, R. B. (1965). The Right of Privacy: Emanations and Intimations. *Mich. L. Rev*, 259-282.

McStay, A. (2017). *Privacy and the Media.* SAGE Publications.

Mehan, J. (2014). *Cyber War, Cyber Terror, Cyber Crime And Cyber Activism.* IT Governance Publishing.

Merriam-Webster, D. (n.d.). *Data*. Retrieved from Dictionary Merriam-Webster: https://www.merriam-webster.com/dictionary/dictionary

Mohammed, M., Khan, M. B., Bashier, E. B. M. (2017). *Machine learning : algorithms and applications.* Boca Raton : CRC Press.

Monino, J.-L.,Sedkaoui, S. (2016). *Big Data, Open Data And Data Development.* Iste.

Morgan, P. (2018). *Machine Learning Is Changing the Rules.* O'Reilly Media, Inc.

Morrison, S. (2019, Dec. 30). *California's new privacy law, explained, The California Consumer Privacy Act gives Californians some control over their data, but only if they know how to take advantage of it*. Retrieved from Vox: https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained

Muoio, D. (2017, Jun 26). *An ex-Tesla exec reveals how the company is transforming itself into a data powerhouse*. Retrieved from Business Insider : https://www.businessinsider.in/an-ex-tesla-exec-reveals-how-the-company-is-transforming-itself-into-a-data-powerhouse/articleshow/59325516.cms

Myatt, G. J., and Johnson, W. P. (2014). *Making Sense of Data I: A Practical Guide to Exploratory Data Analysis and Data Mining, 2nd Edition.* Wiley.

Myers, F. (2019, Jun. 14). *AI: inhuman after all? Joanna Bristol on what the world gets wrong about robots and AI*. Retrieved from Spiked: https://www.spiked-online.com/2019/06/14/ai-inhuman-after-all/

Negley, G. (1966). Philosophical views on the Value of Privacy, 31. *Law and Contemporary Problems*, 319-325.

Netflix Research (n.d.). *About.* Retrieved from Netflix research: https://research.netflix.com/research-area/analytics

Ng, A. (2019, Jun. 5). *Amazon's helping police build a surveillance network with Ring doorbells, Its popular Ring smart doorbells mean more cameras on more doorsteps, where surveillance footage used to be rare*. Retrieved from Cnet: https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/

Ning, S., and Wu, H. (2019, Mar. 07). *China: Data Protection 2019.* Retrieved from ICLG: https://iclg.com/practice-areas/data-protection-laws-and-regulations/china

Noordyke, M. (2019, Apr. 18). *US state comprehensive privacy law comparison US state comprehensive privacy law comparison*. Retrieved from IAPP : https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison

NVIDIA (n.d.). *Self-Driving Cars, Driving innovation: Building AI- Powered Self Drivers Cars,.* Retrieved from NVIDIA: https://www.nvidia.com/en-us/self-driving-cars/

OASIS (2012). *The Consultative Committee For Space Data Systems, Recommendation For Space Data System Practices – Reference Model For An Open Archival Information System (OASIS).* Magenta Book.

OECD (2013). *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and TransBorder Flows of Personal Data.* OECD.

OECD (n.d.). *Wo we are*. Retrieved from OECD: https://www.oecd.org/about

ORWELL, G. (2020). Otbebookpublishing.

Parisi, A. (2019). *Hands-On Artificial Intelligence for Cybersecurity.* Packt Publishing.

Pasquale, F. (2019). Data-Informed Duties in AI Development,. *Colum. L. Rev*, 1917-1940.

Patel, N. (n.d.). *How Google's Search Engine Really Works (A Peek Under the Hood)*. Retrieved from Neil Patel: https://neilpatel.com/blog/how-google-search-engine-really-works/

Perez, E., Hume, T. (2016, Feb). *Apple opposes judge's order to hack San Bernardino shooter's iPhone*. Retrieved from https://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html

Phelps, J., Nowak, G., Ferrel, E. (2000). Privacy Concerns And Consumer Willingness To Provide Personal Information. *Public Policy & Marketing*, 27-41.

Postman, N. (2013, Dec. 1). *Technology: Informing Ourselves to Death, A speech given to Gesellschaft fü Informatik. Stuttgart, Germany (Oct. 1990).* Retrieved from Memorian Press: https://www.memoriapress.com/articles/informing-ourselves-death/

Pozen, D. E. (2016). Privacy-Privacy Tradeoffs. *U. Chi. L. Rev*, 221-247.

Preston, A. (2014, Aug. 03). *The Death of privacy Google knows what you're looking for. Facebook knows what you like. Sharing is the norm, and secrecy is out. But what is the psychological and cultural fallout from the end of privacy?* Retrieved from the guardian: https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

Prosser, W. L. (1960). Privacy. *Calif. L. Rev.* , 383-423.

Prusty, N. (2018). *Blockchain For Enterprise.* Packt Publishing.

Ramgir, M. (2019). *Internet Of Things: Architecture, Implementation And Security* . Pearson .

Raul, A. C. (ed.) (2017). *The Privacy, Data Protection And Cybersecurity Law Review.* Gideon Roberton.

Rodden, J. (2006). *Every Intellectual's Big Brother : George Orwell's Literary Siblings.* University of Texas Press.

Rosner, G. (2016). *Privacy and the Internet of Things.* O'Reilly Media, Inc.

Rouse, M. (ed.) (n.d.). *Definition Encryption*. Retrieved from TechTarget: https://searchsecurity.techtarget.com/definition/encryption

Rubinoff, S. (2020). *Cyber Minds.* Packt Publishing.

Sadowski, J. (2016, Aug. 31). *Companies are making money from our personal data –but at what cost? Data appropriation is a form of exploitation because companies use data to create value without providing people with comparable compensation*. Retrieved from The Guardian : https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon

Sainato, M. (2020, Feb. 5). *'I'm not a robot': Amazon workers condemn unsafe, grueling conditions at warehouse*. Retrieved from The guardian: https://www.theguardian.com/technology/2020/feb/05/amazon-workers-protest-unsafe-grueling-conditions-warehouse

Salinas, S. (2018, Oct. 8). *A Google bug exposed the information of up to 500,000 users*. Retrieved from CNBC: https://www.cnbc.com/2018/10/08/google-bug-exposed-the-information-of-up-to-500000-users.html

Sawers, P. (2020, Jan 10). *Chinese Court rules AI-Written article is protected by copyright*. Retrieved from venturebeat: https://venturebeat.com/2020/01/10/chinese-court-rules-ai-written-article-is-protected-by-copyright/

Schmelzer, R. (2019, Oct. 24). *AI and Blockchain: Double the Hype or Double the Value?* Retrieved from Forbes: https://www.forbes.com/sites/cognitiveworld/2019/10/24/ai-and-blockchain-double-the-hype-or-double-the-value/#921e4365eb41

Schneier, B. (2016). *Data And Goliath: The Hidden Battles To Collect Your Data And Control Your World.* W. W. Norton & Company.

Seely, S. (2016, May 02). *The Amazon flywheel: part 1*. Retrieved from Sam Lee blog: http://www.samseely.com/blog/2016/5/2/the-amazon-flywheel-part-1

Segal, A. (2017). Bridging the Cyberspace Gap: Washington and Silicon Valley. *PRISM*, 66-77.

Shi-Kupfer., Ohlberg, M. (2019). *China's Digital Rise Challenges for Europe.* Merics Papers on China.

Silver, D., and Hassabis, D. (2017, Oct. 18). *AlphaGo Zero: starting from scratch*. Retrieved from DeepMind: https://deepmind.com/blog/article/alphago-zero-starting-scratch

Simon, M. (2019, Jul. 29). *Apple's Siri 'eavesdropping' controversy can be fixed with a toggle that should've been there all along*. Retrieved from Macworld: https://www.macworld.com/article/3411992/apple-siri-eavesdropping-controversy-privacy-toggle.html

Singer, N. (2018, Apr). *What do Don't Know About How Facebook Uses Your Data*. Retrieved from New York Times : https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

Solove, D. J. (2004). *The Digital Person: Technology And Privacy In The Information Age.* N.Y.U. Press.

Solove, D. J., Rotenberg, M., Schwartz, P. M. (2006). *Information privacy law.* New York, NY: Aspen Publishers.

Sparks, E. (2019, Nov. 24). *AI Leadership and the Positive Impacts on Economy, Privacy, Environmental Health*. Retrieved from Forbes: https://www.forbes.com/sites/evansparks/2019/11/14/ai-leadership-and-the-positive-impacts-on-economy-privacy-environmental-health/#2bd55f1f327e

Spindler, G. (2019). Copyright Law and Artificial Intelligence. *International Review of Intellectual Property and Competition Law volume* , 1049-1050.

Spitznagel, E. (2020, Jul. 13). *Inside the hellish workday of an Amazon warehouse employee*. Retrieved from New York Post: https://nypost.com/2019/07/13/inside-the-hellish-workday-of-an-amazon-warehouse-employee/

Starling, W. (2019). *Information Privacy Engineering And Privacy By Design: Understanding Privacy Threats, Technology, And Regulations Based On Standards And Best Practices.* Addison-Wesley Professional.

Statt, N. (2019, Mar. 6). *How Artificial Intelligence Will Revolutionize the Way Video Games Are Developed and Played: The advances of modern AI research could bring unprecedented benefits to game development.* Retrieved from The Verge: https://www.theverge.com/2019/3/6/18222203/video-game-ai-future-procedural-generation-deep-learning

Stephenson, D. (2018). *Big Data Demystified: How To Use Big Data And Data Science To Make Better Business Decisions And Gain Competitive AdvantagE.* FT Publishing International.

Stute, D. J. (2015). Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD. *Michigan Journal of International Law,* 649-679.

Sullivan, E. T. (2019). *Understanding Antitrust And Its Economic Implications.* Carolina Academic Press.

Sundblad, W. (2018, Oct 18). *Data Is The Foundation For Artificial Intelligence and Machine Learning*. Retrieved from Forbes: https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/#a18ff4f51b49

Sussman., H. E. (2020, Feb. 13). *California Attorney General Releases Updated Drafts of Proposed CCPA Regulations*. Retrieved from Orrick Blog: https://blogs.orrick.com/trustanchor/2020/02/13/california-attorney-general-releases-updated-drafts-of-proposed-ccpa-regulations/

Sweeney, L. (2002). k-Anonymity: A Model for Protecting Privacy1. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 557-570.

Szczepański, M. (2019). *Economic impacts of artificial intelligence (AI).* Economic impacts of artificial intelligence (AI).

Takyar, A. (2020, Feb. 24). *Blockchain and AI- Towards the "Forth Industrial Revolution"*. Retrieved from LeewayHertz: https://www.leewayhertz.com/blockchain-and-ai/

Tanner, A. (2014). *What stays in Vegas : the world of personal data lifeblood of big business and the end of privacy as we know it* . PublicAffairs

Taulli, T. (2019). *Artificial Intelligence Basics: A Non- Technical Introduction.* Apress.

Taylor, R., and Kelsey, T. (2016). *Transparency And The Open Society – Practical Lessons For Effective Policy.* Bristol University Press.

Temple, C. (2019, Sept. 11). *AI-Driven Decision-Making May Expose Organizations to Significant Liability Risk*. Retrieved from Corporate Compliance Insights: https://www.corporatecomplianceinsights.com/ai-liability-risk/

The IAPP Westin Research Center. (n.d.). *Download "Top 5 Operational Impacts of the California Consumer Privacy Act" CCPA*. Retrieved from Iapp: https://iapp.org/l/ccpagd/?gclid=EAIaIQobChMI38jOsLo5wIVFP5kCh1JSQcnEAAYAiAAEgKVU_D_BwE

The National Security Commission. (n.d.). *About*. Retrieved from ncsai: https://www.nscai.gov/about

Official U.S. government information about the Global Positioning System (2020, Apr. 22). *What is GPS?* Retrieved from GPS.GOV: https://www.gps.gov/systems/gps/

Trepp, P. (2020, Jan 7). *How Face Recognition Evolved Using Artificial Intelligence*. Retrieved from Facefirst: https://www.facefirst.com/blog/how-face-recognition-evolved-using-artificial-intelligence/

Trivedi, V. (2019). *How to Speak Tech: The Non-Techie's Guide to Key Technology Concepts.* Apress.

Turing, A. M. (1950). Computing Machinery and Intelligence. *MIND A Quarter Review of Psychology and Philosophy*, 433-460.

Uber. (n.d.). *How to use the Uber app*. Retrieved from Uber: https://www.uber.com/us/en/about/how-does-uber-work/

United Nations. (2019). *Shaping our Future Together – Universal Declaration of Human Rights* . Retrieved from United Nations: https://www.un.org/en/universal-declaration-human-rights/

UNCTDA, U. N. (2016). *Data protection regulations and international data flows: Implications for trade and development*. Retrieved from UNCTDA: https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

Vincent, J. (2019, Mar. 15). *Facebook promises new AI tool will proactively detect revenge porn*. Retrieved from The Verge: https://www.theverge.com/2019/3/15/18266974/facebook-instagram-revenge-porn-ai-filter

Vincent, J. (2019, Mar 6). *Google is making it easier for AI developers to keep user's data private*. Retrieved from The Verge: https://www.theverge.com/2019/3/6/18253002/google-ai-data-privacy-tensorflow-differential-module-code

Wagner, J. (2017, Jun. 01). *China's Cybersecurity Law: What You Need to Know*. Retrieved from The Diplomat: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

Waldo, J., Lin, H. S., and Millett, L. I. (2007). *Engaging Privacy And Information Technology In A Digital Age*. Nat'l Academies Press.

Walsh, F. (2020, Jan 2). *AI' outperforms' doctors diagnosing breast cancer*. Retrieved from BBC News : https://www.bbc.com/news/health-50857759

Wang, H. (2011). *Protecting Privacy In China, A Research On China's Privacy Standards And The Possibility Of Establishment The Right To Privacy And The Information Privacy Protection Legislation In Modern China.* Springer.

Warren, S. D., Brandeis, L. D. (1890). The Right to Privacy. *HARV. L. REV*, 193-220.

West, D. M. (2011). *Using Digital Technology To Further Social And Political Innovation.* Brookings Institution Press.

Wilson, H. J., and Daugherty, P. R. (2018). *Human + Machine : Reimagining Work in the Age of AI.* Harvard Business Review Press.

Wilson, N. (2019, Jun). *Reduced Demand Uncertainty and the Sustainability of Collusion: How AI Could Affect Competition.* Retrieved from Federal Trade Commission: https://www.ftc.gov/reports/reduced-demand-uncertainty-sustainability-collusion-how-ai-could-affect-competition

Winter, D. (2018, Jun 19). *AI Errors vs. Human Errors*. Retrieved from International Director: https://internationaldirector.com/technology/ai-errors-vs-human-errors/

WIPO. (n.d.). *WIPO Paris Convention for the Protection of Industrial Property,*. Retrieved from WIPO Portal: https://wipolex.wipo.int/en/text/287556

Yang, H. S. (. (2019). *China, in The Privacy, Data Protection And Cybersecurity Law Review.* Tom Barnes.

Yelpaala, K. (2018). *International Business Transactions.* Mcgeorge School Of Law.

YouTube. (n.d.). *What is YouTube*. Retrieved from YouTube: ttps://edu.gcfglobal.org/en/youtube/what-is-youtube/1/

Yu, C. (2020, Mar. 26). *China ahead of US, EU in AI and Data privacy, experts says*. Retrieved from ChinaDaily.com: http://www.chinadaily.com.cn/a/201903/26/WS5c99b620a3104842260b29b8.html

Zalta, E. N. (ed.) (2019, Oct. 30). *Privacy and Information Technology.* Retrieved from Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/it-privacy/#toc

Zhang, L. (2019, Jun 06). *Trade Secret Provisions under Anti-Unfair Competition Law Revised,* . Retrieved from The Law Library of Congress, Global Legal Monitor : https://www.loc.gov/law/foreign-news/article/china-trade-secret-provisions-under-anti-unfair-competition-law-revised/

Zhu, Q. (2019, Jun. 25). *Data Research: Compliance with Cross-Border Personal Data Transfer Limitations*. Retrieved from Lexology : https://www.lexology.com/library/detail.aspx?g=7dff1512-40ab-4614-a3fe-f435a5b7a37f

Zhu, T., Li, G., Zhou, W. Yu, P. (2017). *Differential Privacy And Application.* Spring.

Cases, directives, and laws

Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208 (2014).

Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014 ECLI: EU: C: 2014:317

Gee v. Pritchard, 2 Swans. 402, 36 Eng. Rep. 670 (1818).

Griswold v. Connecticut, 381 U.S. 479 (1965).

Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S 340 (1991).

Prince Albert v. Strange, 2 De G. & Sm. 652, 41 Eng. Rep. 1171, 1 Mac. & G. 25, 64 Eng. Rep. 293 (1849).

Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.

Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012 (326/159).

Declaration of Independence (U.S. 1776).

DIRECTIVE (EU) 2016/943, art.2, 2016 O.J. (L 157/1).

CAL. CIV. CODE § 1798.105(a) (West 2018).

CAL. CIV. CODE § 1798.140(c) (1) (West 2018).

CAL. CIV. CODE § 1798.140(c) (2) (West 2018).

Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

G.A.Res.217 (12) A, Universal Declaration of Human Rights (Dec.10.1948).

Justices of the Peace Act 1361, 34 Edw. 3, c. 1. (Eng.).

Patent Law of the People's Republic of China, article 22, http://english.sipo.gov.cn/lawpolicy/patentlawsregulations/915574.htm

REGULATION (EU) (GDPR) 2016/679, art. 17, 2016 O.J. (L 119/43).

REGULATION (EU) No 235/2014, 2014 O.J (L77/92).

Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), NEW AMERICA (2018),

https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, (last visited Jan 21, 2020).

U.S. Copyright Law, Copyright Law of the United States (tittle 17), Copyright.gov (Dec. 2016).

U.S.C.A §101 (2017).

18 U.S.C.A. § 1839 (2018).

18 U.S.C. § 2721 (1994).