The Role of Data Protection and Cybersecurity Regulations in Artificial Intelligence Global Governance: A Comparative Analysis of the European Union, the United States, and China Regulatory Framework

By Dalia Alic

In Partial Fulfillment of the Requirements for the Master of Arts in Human Rights

Master of Arts in Human Rights Final Thesis

SUPERVISOR: Professor Cameran Ashraf, Ph.D.

Central European University

Vienna, Austria

June 2021

TABLE OF CONTENTS

ABSTRACT

Global challenges brought with artificial intelligence require joint, global solutions in order to be successfully tackled. This is important for setting up an ethical and human rights-focused precedent in the future of global governance on emerging technologies and for proper safeguarding of human rights on the international level. However, in order to achieve this, a global framework for artificial intelligence should be harmonized in the form of a consensus on the global approach to AI, despite differences in understanding data protection as a human right and level of prioritization cybersecurity of the big data as a necessary security measure to protect personal information which feeds AI.

This thesis provides a comparative overview of similar legal and policy patterns with detected similarities of regulatory patterns of the EU, the US, and China relevant for data privacy and security in the age of AI, which could serve for further research on setting up a global, ethical AI governance that transcends over cultural, legal and political differences in understanding human rights in order to safeguard rights of the newer generation.

Cultural, legal, and policy settings of three leading AI global players are examined by identification, mapping, and comparison of (1) the key legal instruments on data protection relevant to safeguarding personal information in artificial intelligence; (2) provisions of national development plans and ethical guidelines (if any) on safeguarding data protection and preserving the security of big data; (3) initiatives and international efforts on achieving a global approach on AI that could benefit human rights and therefore prioritize safeguarding data protection on the global level. The research finds that the EU, the US, and China surprisingly share certain similarities within their legal and policy regulatory frameworks despite cultural and political differences, starting from facing similar challenges in the AI regulation in the context of data privacy and security, soft law versus hard law challenges, to normative aspirations and global AI leadership.

Keywords: Artificial Intelligence ▪ Human-centric AI ▪ Data Protection ▪ Cybersecurity ▪ Global Governance ▪ Transnational Lawmaking ▪ Regulatory Framework ▪ European Union ▪ United States of America ▪ China

ACKNOWLEDGMENTS

Firstly, I would love to thank my family and friends for their incredible support, especially to my mother Antonija, father Sead, and partner Ivan for their unconditional support and for granting me the opportunity to prioritize my education - I am beyond grateful for all their help.

My deepest gratitude goes to my supervisor, Professor Cameran Ashraf, who taught me that human rights start with small steps, encouraged me to always ask the right questions and supported my curiosity for exploring global governance and human rights in emerging technologies – I will cherish all our productive discussions and gained knowledge about life.

I would like to express my appreciation to Professor Marie-Pierre Granger, who helped me reveal my passion for transnational law, inspired me to always go the extra mile, and gave me the courage to tackle challenging academic and legal topics successfully.

I am grateful to the Head of Department, Professor Mathias Möschel, for the consistent support, encouragement, and kindness shown during the challenging academic year spent in the pandemic.

Furthermore, special thanks go to Professor Zsuzsanna Tóth from Center for Academic Writing and Gail Aguilar from Thesis Buddy Program for being my lighthouse in the thesis writing process, as well as Cezara-Alexandra Panait for sharing her valuable experience and knowledge in artificial intelligence and digital policy that inspired me to further explore this topic.

My kind gratitude goes to my dear friends and colleagues Hanh Linh, Ferowza, Veronica, Monty, and Marton for time spent together and for founding and leading European Horizons CEU student-led policy lab side by side with me in order to enable CEU students opportunities for academic publishing and further policy explorations.

Lastly, I am grateful to CEU, together with all its faculty members and staff, for having the opportunity to expand my knowledge in human rights legal studies and to CEU Alumni Office for being selected as an Alumni Scholarship Recipient.

LIST OF ABBREVIATIONS

AHEG	Ad Hoc Expert Group (UNESCO)
AI	Artificial intelligence
AIDP	New Generation Artificial Intelligence Development Plan (China)
CCPA	California Consumer Privacy Act (US)
CoE	Council of Europe
CSL	Cybersecurity Law of the People's Republic of China
ENISA	European Union Agency for Cybersecurity
EU	European Union
G20	Group of Twenty
GDPR	General Data Protection Directive (EU)
GPAI	Global Partnership on Artificial Intelligence
IA-AI	International Alliance for a Human-Centric Approach to Artificial Intelligence
ICCPR	International Covenant on Civil and Political Rights
ML	Machine learning
OECD	The Organisation for Economic Co-operation and Development
R&D	Research and development
SDG	Sustainable Development Goals (UN)
TEU	Treaty on European Union
TFEU	Functioning of the European Union
UDHR	Universal Declaration on Human Rights
UN	United Nations
UNESCO	United Nations Educational, Scientific, and Cultural Organization
US	United States
WEF	World Economic Forum

INTRODUCTION

"*AI technologies have the capacity to do a lot of good in the world, but whether they do so is highly dependent upon both how we use and build those AI technologies in the first place*."[1]

Data privacy and security will be the most crucial issue in this decade.[2] The global race for developing artificial intelligence (AI) is ongoing. Furthermore, according to Moore's Law, simply put together, it is predicted for decades that the size of the data (chip density) doubles every two years. Roughly said, this would mean that this exponential growth of data doubles almost every two years, creating quintillions of bytes of data every day.[3] This statistic requires attention from policymakers as the enormous amount of data produced every day is not making the task of keeping it secure and private any easier.

Global challenges require global and joint solutions - in order to successfully safeguard data protection and cybersecurity of big data in the age of AI and emerging technologies, a global joint effort should be made to provide standardized legally binding frameworks, technological regulations, and digital policies not just to prevent possible human rights violations such as the right to privacy in the context of data protection and cybersecurity of big data, but to encourage initiatives, frameworks, programs, and projects both in policy-making and business sphere to achieve SDGs and human-centric AI. However, certain challenges arise when the debate takes over if such policies and frameworks should be law-binding and if strict regulations could affect innovation progress, yet a decision has to be made if the right to privacy as a human right will be sacrificed in the AI arms race. In addition to this, another issue for

[1] Cohen, 'The Ethical Use of Personal Data to Build Artificial Intelligence Technologies: A Case Study on Remote Biometric Identity Verification'.
[2] Meehan, 'Data Privacy Will Be The Most Important Issue In The Next Decade'.
[3] Moore, 'Cramming More Components onto Integrated Circuits'.

achieving global governance on AI rises with the difference in cultural values, innovation, and industry versus human rights prioritization, evident in the leading AI trendsetters: the EU, the US, and China.

This paper primarily examines data protection and cybersecurity regulatory frameworks of the EU, the US, and China and identifies similar patterns that could be a relevant basis for the creation of ethical AI global governance by mapping and comparing the critical national and international legal and policy instruments with possible implications in the context of safeguarding personal information in artificial intelligence. Therefore, the purpose of this thesis research is to understand the legal and policy framework positioning of data protection and the cybersecurity of the data in the supply chain of AI, and precisely the big data consisted of personal data in jurisdictions of the EU, the US and China to understand how it could impact the likeliness of setting up the joint global AI agenda and governance. This research hopes to contribute to the existing knowledge in the law discipline by addressing the specific issue of data protection and cybersecurity of AI by putting it in the causational relation to the global AI agenda.

METHODOLOGY

This thesis will aim to provide an overview of the situation by basing the research on the following central question:

- Which are similarities in the data protection and big data cybersecurity regulatory patterns of the EU, the US, and China relevant for artificial intelligence that could ethical, global AI agenda in the context of privacy be built on?

The research question focuses on the identification of similar patterns in the AI regulatory framework of the current key AI trendsetters and if AI can be seen as a tool of cohesion due to joint multilateral efforts on creating a global ethical AI regulatory framework/agenda which could serve as a precedent for global governance on emerging technologies, despite differences in specific human rights standards such as data protection and cybersecurity of big data.

In order to get necessary insights for the main questions, the thesis research includes several sub-questions, which will be individually covered in the thesis chapters:

- How is the interconnection of the data protection, cybersecurity of the big data, and current global initiatives on AI relevant for the global AI agenda and ethical governance;
- What are the key domestic and international legal and policy instruments in the EU, the US, and China when it comes to data protection that will be challenged with the implications brought by the AI, and how do they differ in the context of the right to privacy and cybersecurity of big data;
- Can international initiatives on artificial intelligence be considered as the first step towards global artificial intelligence agenda and governance?

Put in simple words, this thesis focuses on three topics (1) data protection; (2) cybersecurity; (3) AI governance and its relations to selected jurisdictions of the EU, the US, and China. Furthermore, for the purpose of this paper, I have selected to focus on principles such as data protection, including its sub-principles being (1) consent; (2) control over the use of data; (3) ability to restrict processing; (4) right to erasure; (5) privacy by design; (6) existing data protection legal, regulatory framework while under the principle of cybersecurity I allude sub-principles such as (1) safety; (2) security; (3) security by design; (4) privacy-preserving methods such as encryption, anonymization, pseudonymization, and minimization.[4]

With the aim of tackling the main question and sub-questions, the paper further examines the key legal and policy instruments on data protection and right to privacy in the jurisdiction of the EU, the US and China will be primarily consulted as well as international treaties the respective countries are a part of. Regulatory frameworks and proposals on data protection and cybersecurity of AI will be researched and mapped, together with the agenda of selected global AI initiatives. As secondary resources, this thesis will consult a variety of scholarly papers, published a comparative analysis of respective jurisdictions in the context of human rights and sovereignty, theoretical papers on human rights and the right to privacy, examinations, and findings on quantum computing and emerging technologies that could directly impact the future of data protection, and more.

Starting with the theoretical analysis of the interconnection between data protection, cybersecurity, and global initiatives on artificial intelligence in Chapter 1., this paper uses primarily the comparative-legal method to compare the EU, the US, and China jurisdictions in Chapters 2., 3. and 4. in (1) selected vital domestic and international legal instruments of data

[4] Inspired by Fjeld et al., 'Principled Artificial Intelligence: MappingConsensus in Ethical and Rights-Based Approaches to Principles for AI'.

protection relevant for artificial intelligence; (2) differences in socio-political context and cultural understanding of the right to privacy which is applied through data protection regulation; (3) national plans, policy framework or already applied development and modification of legal instruments to address artificial intelligence and other emerging technology. This legal analysis will provide an overview of the national/supranational priority (e.g., human rights, economy, and industry, national security), including the awareness of data protection prioritization. Of course, constitutions of selected jurisdictions will be briefly analyzed as well, since as a primary law, a constitution is a fundamental rule upon which cultural values and relations of the state and people are regulated: "the values reflected in the constitution are codified in the form of primary law and offer important guidance for making laws and policies and regulating the actions of the government."[5]

In Chapter 5., the interdisciplinary theoretical approach will discuss the legal, cultural, and political importance, opportunities and limitations for global AI governance, and the importance of international AI initiatives. A slightly different type of comparison will be applied to examine selected international artificial intelligence initiatives with theoretical analysis of socio-political and cultural context when it comes to the right to privacy and prioritizing as well as safeguarding human rights in AI to determine if normative powers of certain jurisdictions can prevail.

The thesis topic covering artificial intelligence and data protection is undoubtedly rewarding in the quality and quantity of available resources. Most of the legal documents, treaties, declarations, reports, research papers, databases, policy frameworks, and national plans included in this thesis are just over a few years old and available in either British or American English language. However, certain key legal instruments, regulatory frameworks,

[5] Ma, Zhao, and Liao, 'The Values Demonstrated in the Constitution of the People's Republic of China'.

and policies of China are unavailable in the official English translation and require unofficial translation tools and resources[6], as my Chinese Mandarin skills are currently not sufficient for fluent legal and academic understanding.

[6] Such as 'China Law Translate', Google Translate or published unofficial translations by specialized international law companies operating in China.

CHAPTER 1. INTRODUCING THE ROLE OF DATA PROTECTION AND CYBERSECURITY IN ARTIFICIAL INTELLIGENCE: INTERCONNECTION WITH CHALLENGES AND OPPORTUNITIES IMPORTANT FOR GLOBAL GOVERNANCE

While there is no universal official definition, Alan Turing stated that once computers (artificial intelligence) will mimic human responses well enough to fool an interrogator and achieve human-level performance in cognitive tasks, intelligent behavior should be seen as artificial intelligence.[7] Machine learning (ML), on the other hand, is a type of artificial intelligence capable of self-learning from data and application of gained 'knowledge – it relies on statistical interference in datasets to identify patterns that are usually unidentifiable to the human eye and to perform specific tasks without the need for human intervention.[8]

Furthermore, the term big data implies "large or complex volumes of data, both structured and unstructured that can be analyzed to bring value"[9] where "the professional literature refers to the four Vs: the Volume of data collected, the Variety of sources, the Velocity with which the analysis of the data can unfold, and the Veracity of the data which could (arguably) be achieved through the analytical process."[10] Therefore, this paper will from now to on mostly explore AI in the context of ML that 'lives' on big data and datasets made of enormous amounts of personal information and its implications within the legal and policy regulatory frameworks of the EU, the US and China, as well as global governance.

"Data is the new oil,"[11] and what was once controlled with oil now is controlled with the data. Lots of data. Moreover, the role of cybersecurity is pivotal when it comes to big data and AI as it is defined as "the organization and collection of resources, processes, and structures

[7] Turing, Alan 'Computing Machinery and Intelligence'.
[8] Russel and Norvig, *Artificial Intelligence: A Modern Approach*.
[9] Gruschka et al., 'Privacy Isssues and Data Protection in Big Data: A Case Study Analysis Under GDPR'.
[10] Marr, 'Why Only One of the 5 Vs of Big Data Really Matters'.
[11] 'The World's Most Valuable Resource Is No Longer Oil, but Data'. The Economist.

used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."[12] It is an essential element of bringing users, citizens, and individuals' trust and confidence in the digital ecosystem.[13] Alternatively, in more simple words – to prevent access to unauthorized parties or tools that could impact digital property: "information security and privacy are intertwined domains within cybersecurity."[14] Unfortunately, very few studies on data protection and even relevant legislation/public policies examined in this study addressed the actual value of cybersecurity per se in the age of big data, despite "increased access to sensitive information that when processed can directly jeopardize the privacy of individuals and violate data protection laws."[15] However, the world slowly realizes the importance of data protection and how misuse can lead to catastrophic events – from the online to the offline world. For instance, by using the data of more than 87 million Facebook profiles of American citizens[16] and creating psychological profiles for the purposes of political advertising, the Republican-funded Cambridge Analytica and its scandal[17] for the 2016 USA Presidential Campaign is just a glimpse of wrongful possibilities in case of the data protection, especially in the big data and AI, if not appropriately safeguarded – technically and by the law.

Another definition of cybersecurity is "the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights"[18] Several studies and case studies examples have proven that although such measures are welcome and needed to protect the identity of data subjects, they might not be enough[19] – re-identification is usually possible.

[12] Tene and Polonetsky, 'Big Data for All'.
[13] Davenport, Harris, and Shapiro, 'Competing on Talent Analytics'.
[14] Ferrándiz and Degli-Esposti, 'After the GDPR'.
[15] Gruschka et al., 'Privacy Isssues and Data Protection in Big Data: A Case Study Analysis Under GDPR'.
[16] Meredith, 'Facebook-Cambridge Analytica'.
[17] Cadwalladr, 'I Made Steve Bannon's Psychological Warfare Tool'.
[18] Craigen, Diakun-Thibault, and Purse, 'Defining Cybersecurity'.
[19] Gruschka et al., 'Privacy Isssues and Data Protection in Big Data: A Case Study Analysis Under GDPR'.

New ways of privacy-preserving methods should be explored, examined and legally implemented in order to prevent casualties in case of a cyberattack impacting databases: "even if directly identifiable parameters are removed from a dataset, if might be possible to re-identify single individuals by combining the dataset with other information (…) this approach for de-anonymization is called background knowledge attack."[20] The rise of emerging technology, such as quantum computing, threatens privacy and seeks privacy-preserving solutions, such as advanced encryption through blockchain that could be proposed and implemented globally only through global AI initiatives or global AI governance focused on safeguarding privacy as a human right. Interestingly, the European Union Agency for Cybersecurity (ENISA) detected a multi-dimensional relationship between cybersecurity and artificial intelligence and described its dimension of interdependency in three categories: cybersecurity for AI, AI to support cybersecurity, and malicious use of AI[21]. In the context of this paper, the cybersecurity aspect will be examined concerning privacy and security protections in the AI supply chain can be protected through, if possible, law-binding regulations as: "although a variety of privacy-preserving mechanisms exist to protect information privacy during the data generation, data storage, and data processing phase, corporations may not always have incentives to adopt these measures."[22] Thus, this paper will rely on ENISA's mapping of the AI Threat Landscape created by using threat modeling and assessment techniques and examine legislations which are, could or should aim better in strengthening cybersecurity element and criteria in the policy context, which is directly related to data protection and global governance in the age of AI as "information security and privacy are intertwined domains within cybersecurity" through

[20] Gruschka et al.
[21] European Union Agency For Cybersecurity, 'AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence'.
[22] Mehmood et al., 'Protection of Big Data Privacy'.

leveraging differential privacy in order to reduce risk manipulation of machine learning models, and which is also represented through applied privacy by design principles."[23]

AI cannot be left for self-regulation, and the fact is that competing for the AI race also means competing in policy and law-making. Among numerous benefits which AI innovation holds for humanity, a careful risk assessment and certain steps should be implemented in order to secure human rights, human security, and humanity all together. There is already "one job where AI has already shown superiority over human beings – hacking,"[24] and there is more to come as AI develops and merges with emerging technology, presenting a new type of danger to social values and constitutional rights[25] as "privacy, anonymity, and autonomy are the main casualties of AI's ability to manipulate choices in economic and political decisions."[26] In other words, AI can reshape the world we know - as Jean Garcia Periche, the CEO of Genia, the public benefit corporation for AI systems in Latin America, wrote:

> "*The impending disruptions coming from Artificial Intelligence (AI), together with the rise of digital surveillance and massive economic inequality, are fundamental threats to the stability of the world order. This realization calls for a new global agenda that is able to manage the increasing complexity of our globalized techno-landscape. For that reason, furthering the multilateral system will require an integrated approach between cognitive technologies and global governance*."[27]

However, human history shows that urgent international actions and agreements are possible when life on Earth is brought into question, and this has been proven with the case of

[23] Ferrándiz and Degli-Esposti, 'After the GDPR'.
[24] '2018 AI Predictions: Eight Insights to Shape Business Strategy'.
[25] Wright, 'How Artificial Intelligence Will Reshape the Global Order'.
[26] Manheim and Lyric Kaplan, 'Artificial Intelligence'.
[27] Periche, 'Artificial Intelligence and the Future of Global Governance'.

environmental endangerment. Montreal Protocol[28], an international treaty designed for urgent protection of the ozone layer after the discovery of the damage caused by industrial chemicals, was signed and ratified by all United Nations Members (197 countries) in just several years with working groups still monitoring and evaluating its effects, while the sovereignty concerns "were held in check by the common concern and precautionary principles."[29] It is known as one of the most, if not the most successful, "single international agreement to date."[30] Years later, the question is if such imperative action is possible in case human rights and democracy are at stake, the last pillars keeping humanity safe from possible future dystopia? On top of that, it is questionable "how much of cyberspace can be positioned as a global common good and what is the way to treat it as such, that is, the appropriate governance."[31] Unlike Montreal Protocol, global governance on AI can bring as equally or more opportunities to humanity than threats if governed and secured carefully. It is not only about preventing possible dystopia but about exploring ways of how AI as the predecessor of emerging technology can grow together with humanity through joint policy frameworks and a careful approach to sovereignty concerns of individual states. It will set up a precedent for the rest of even more disruptive technology such as quantum technology or even outer space-related concerns that will require unity and quick reaction of all countries united despite political tensions, cultural differences, and more. In the end, the world, our planet, is a global village[32], and communication seems indeed like the best way of solving global challenges without violating human rights, as global problems usually require global solutions.[33]

To conclude the chapter, now more than ever before, data protection and cybersecurity of big data consisting of personal information should arise on lawmaking and policymaking

[28] United Nations Treaty Collection, Montreal Protocol on Substances that Deplete the Ozone Layer.
[29] Green, 'Lessons Learned from the Montreal Protocol'.
[30] Wassenhoven, 'The Montreal Protocol on Substances That Deplete the Ozone Layer'.
[31] Timmers, 'Ethics of AI and Cybersecurity When Sovereignty Is at Stake'.
[32] McLuhan and Powers, *The Global Village: Transformations in World Life and Media in the 21st Century*.
[33] Periche, 'Artificial Intelligence and the Future of Global Governance'.

agendas – and global initiatives on AI, as the first step towards global AI governance, can play an important role. Hence, this interconnection is crucial, mainly as a new emerging technology develops, thus bringing global challenges that can be answered only with joint, united actions despite differences in cultural values or innovation regulations.

PART I. COMPARATIVE LEGAL AND POLICY ANALYSIS IN THE CONTEXT OF DATA PROTECTION AND BIG DATA CYBERSECURITY: THE EU, THE US, AND CHINA

The first part of the thesis aims to provide the overview of the comparative analysis that will be conducted on the three selected and observed jurisdictions to understand some of the main differences within regulatory frameworks relevant to AI as well as the cultural, political, and social values driving the selected legal and policy documents.

In order to understand how the most influential players in the AI race understand the importance of data protection, selected metrics for comparison are further: (1) legal instruments relevant for data protection and their type; (2) scope and level of legal protection; (3) special observatory boards for data protection and privacy responsible for their overseeing the law or data protection and privacy violations as a human right; (4) socio-political and cultural context behind the legislation with the elements of the cultural anthropology applied analysis.

Conducting such a comparative approach of legal instruments is setting up the crucial base before further understanding and comparing AI development plans and policy and regulatory implications on data protection and cybersecurity of big data. Understanding the differences in the context of the right to privacy is one of the essential steps when speaking of safeguarding human rights in the AI globally, and by understanding the nature of differences in three cultures that are leading the AI race is the key to transcendence the collaboration on the global level.

CHAPTER 2. JURISDICTION OF THE EUROPEAN UNION

2.1. Cultural Values Presented in the Constitution: Positioning and Understanding The Right to Privacy

The European Union is not ashamed to highlight how human rights are an essential part of the European identity and among the highest priorities of the ruling. Human rights and citizen's rights are a fundamental part of the European Union and European Union identity[34], consisted even in some of the constitutional documents and important legislations such as the Charter of Fundamental Rights of the European Union[35] (the Charter), the Treaty of the Functioning of the European Union (TFEU)[36] and the Treaty on European Union (TEU) and from the policy on the other hand, through guidelines, recommendation and ethical frameworks such as White Paper on Artificial Intelligence[37], Ethics Guidelines for Trustworthy AI[38], Artificial Intelligence for Europe[39], Coordinated Plan on Artificial Intelligence[40] the Proposal for a Regulation on a European approach for Artificial Intelligence[41] and other. As a supranational entity[42] focused on safeguarding human rights with legally binding regulations, the European Union, in this sense, can fully represent the direction of its member states, thus

[34] "*The European Union (EU) believes that the promotion and protection of human rights around the world is a legitimate concern of the international community. The European Union is bound by its Treaty to promote human rights, democratization and development. The universality, interrelation and indivisibility of human rights, including civil, political, economic, social and cultural rights, as reaffirmed by the 1993 World Conference on Human Rights in Vienna, is the central principle guiding its actions.*" See more: 'Pamphlet No. 14 of the United Nations Guide for Minorities: The European Union: Human Rights and the Fight Against Discrimination'.
[35] Charter of Fundamental Rights of the European Union (2007/C 303/01).
[36] Article 16(1) of the European Union, Treaty on the Functioning of the European Union.
[37] European Commission, 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust'.
[38] European Commission, 'Ethics Guidelines for Trustworthy Artificial Intelligence'.
[39] European Commission, 'Communication from the European Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Coordinate Plan on Artificial Intelligence'.
[40] European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe'.
[41] European Commission, Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.
[42] Kimmo, 'The European Constitution in the Making'.

being compatible for thesis research and comparative study. Thus, with its human rights approach in regards to data protection, "the EU's data protection laws have long been regarded as a gold standard all over the world."[43]

The Charter is essential for its introduction to the 'third generation' of fundamental rights such as data protection, guarantees on bioethics, transparent administration, thus showing the will to understand the need to modify the core legislation of the supranational level in order to approach modern justice and challenges as rightful as possible.[44] While recognizing the difference between the rights to privacy (respect for private and family life) and later introduced protection of personal data, the Charter provides recognition and protection for both[45] through Article 7 that recognizes the respect for private and family life, home and communications, and Article 8 protection of personal data.

For the purpose of the comparison and the legal analysis, two EU legal instruments will be selected and primarily analyzed: (1) Charter of Fundamental Rights of the European Union (the Charter); (2) General Data Protection Directive[46] (GDPR). In addition, the complete understanding of the European Union framework on data protection can also be further understood by examining ePrivacy Directive[47], Police Directive[48] , and the Proposal for the Data Governance Act[49].

[43] 'The History of the General Data Protection Regulation | European Data Protection Supervisor'.
[44] 'Why Do We Need the Charter?'
[45] González Fuster and Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right'.
[46] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[47] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[48] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[49] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).

2.2. EU Regulatory Framework Through the Prism of Data Protection and Cybersecurity Relevant for AI

2.2.1. *Legal Regulatory Framework*

The power of the Charter lies in the fact that it is powerful as it "holds the same status as the EU treaties upon which the entire EU legal system is based[50]" and has to be recognized by the Member States' constitutions[51]. Giving human rights such high status as a priority only cements how important human rights are to this supranational power, which could only have one logical continuation of the same approach to artificial intelligence and other emerging technology. Legally-binding[52] and proclaimed by the European Parliament, the Council and the Commission, the Charter has to be integrated within the bodies and institutions of the EU while respecting the principle of subsidiarity[53] with the obvious right for a remedy if the rights given by the Charter are violated. It is compatible and consistent with the European Convention on Human Rights[54] as their scope of protection and meaning are the same, while the Charter applies to matters only concerning the scope of the EU law[55] and is interpreted by the Court of Justice of the European Union (CJEU).[56]

As previously briefly mentioned, the Charter implements Article 8 on data personal data protection, which provides more details of the scope and level of protection as (1) everyone has the right to the protection; (2) personal data should be processed 'fairly' and only for 'specified' purposes or in the cases of the person's consent or other legitimate bases, such as

[50] Ros, 'The Good, the Bad and the Ugly Arguments for Ditching the EU Charter of Fundamental Rights'.
[51] Chapter VII, General Provisions, Article 53 Level of Protection of Charter of Fundamental Rights of the European Union (2007/C 303/01).
[52] The Charter became legally-binding with the Treaty of Lisbon entering into force in December 2009. See: Craig and Búrca, *EU Law*.
[53] Chapter VII. General Provisions Article 51 of Charter of Fundamental Rights of the European Union (2007/C 303/01).
[54] Preamble and Chapter VII. General Provisions Qarticle 52 of Charter of Fundamental Rights of the European Union (2007/C 303/01).
[55] Groussot, Pech, and Petursson, 'The Scope of Application of Fundamental Rights on Member States' Action'.
[56] 'Equality and Human Rights Commission: What Is the Charter of Fundamental Rights of the European Union?'

law enforcement, etcetera; (3) following these rules and its compliance shall be controlled by an 'independent authority.' It can be added that this separation and development of the privacy phenomena and data protection was an advanced step of what the European Convention of Human Rights did by recognizing but not separating the personal data protection under the right to the private life of an individual.[57]

The General Data Protection Regulation[58] (GDPR) is, put in simple words, the result of efforts to "overcome the fragmented application of Directive 95/46/EC and harmonize data protection norms within the EU digital single market."[59] As a directive, GDPR was enforced as a law in all member states simultaneously[60] while introducing the broad scope of guaranteeing strong personal data protection that could serve as an example to the rest of the world. Firstly, it protects the personal data[61] of individuals by giving them control over their data. Secondly, by having a harmonized regulation across the EU and EEA, it simplifies the regulatory environment for legal entities as well as international businesses, thus offering more robust protection regardless for individuals regardless of their citizenship or residence as the regulation applies to any enterprise that processes the information within the EEA.

This scope shows the true nature of the integration of human rights within the EU, and also respects the wish of more than 90% of European Union citizens who stated in one study that "they want the same data protection rights across the EU and regardless of where their data

[57] "*The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence*". See: S. and Marper v. the United Kingdom (2008) ECHR.
[58] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[59] Ferrándiz and Degli-Esposti, 'After the GDPR'.
[60] Steiner, Woods, and Twigg-Flesner, *EU Law*.
[61] „'Personal data means any information relating to an identified or identifable natural persons ('data subject')." Definitions in Article 4 of the GDPR.

is processed."[62] In addition to this, the member states who cause certain breaches within the law will be sanctioned – this includes companies as well. However, despite the fear of the restrictions coming from the private sector, the GDPR clearly states in Article 1 within the General provisions of Chapter 1 that the main objectives of the Directive are the "protection of natural persons with regard to the processing of personal data"[63] including "the free movement of data"[64] which should "neither be restricted nor prohibited"[65] were not needed.

When it comes to the material scope, GDPR applies for processing[66] the personal data executed by "wholly or partly by automated means"[67], including covering all personal data intended for automated filling system or being a part of such system. The territorial scope of the protection, as previously mentioned, covers the territorial scope that includes the "establishment of a controller or a processor in the Union"[68] even if the processing of the data is done within the Union or not, as defined in Article 3. For the cross-border processing, Chapter 5 of the GDPR defines ways in which such transfers can take place, generally based on an adequacy Decision as in Article 45 with further details on assessing the adequacy depending on the level of protection, assessing the existing and functioning independent supervisory authority in the third country and international commitments the third country has entered or is a part of.

GDPR understands implementation and overseeing of the Regulation seriously as Article 51 includes establishing and preserving the independent status of the supervisory

[62] 'Final Report for the European Commission: Fundamental Rights Review of the EU Data Collection Instruments and Programmes'.
[63] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[64] Ibid.
[65] Ibid.
[66] „Processing means any operation or set of operations which is performed on personal data or on sets of personal data (...)" Definitions in Article 4 of the GDPR.
[67] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[68] Article 3 of the GDPR.

authority/boards, not just on the EU level, but making it through the article mandatory for all EU member states. Therefore, the protection of the data often relies on the powers of Data Protection Authorities who, at least in the European Union, have increased powers under GDPR and can "impose a temporary or definitive limitation including a ban on processing, which will effectively shut organizations down altogether."[69]

Furthermore, initiated by the GDPR, the European Data Protection Board is "composed of the head of one supervisory authority of each Member state"[70] with the tasks such as monitoring the implementation and correct application of the Regulation, advising the Commission, examining questions of the Regulation, drawing up and issuing guidelines for supervisory authorities, reviewing the practical applications of guidelines, promoting the effective bilateral and multilateral collaboration and exchanges, maintaining a publicly accessible register of decisions, and much more, as described in Article 70 in the Tasks of the Board in order to rightfully protect personal data and the implementation of the Regulation across the EU. Besides overseeing data protection rules, it provides 'guidance on key concepts of the GDPR and the Law Enforcement Directive, advising the European Commission on issues related to the protection of personal data and new proposed legislation in the European Union, and adopting binding decisions in disputes between national supervisory authorities."[71]

Additionally, the Police Directive is an essential addition to the GDPR, where the rules of governing personal data are entering the field and activities of law enforcement, investigative bodies, and national security. Unlike GDPR, the Police Directive "requires states

[69] Ferrándiz and Degli-Esposti, 'After the GDPR'.
[70] Article 68 of the GDPR.
[71] "*The EDPB is composed of the representatives of the national data protection authorities of the EU/EEA countries and of the European Data Protection Supervisor. The European Commission participates in the activities and meetings of the Board without voting right. The secretariat of the EDPB is provided by the EDPS. The secretariat performs its tasks exclusively under the instructions of the Chair of the Board*„ See: 'European Data Protection Board: Who We Are'.

to pass an implementing legislation"[72] due to the fact that regulations have the binding legal force that should be applied within the EU. At the same time, directives are legislative acts that provide more 'freedom' for countries to regulate achieving proposed goals within the national regulatory framework: "it is up to the individual countries to devise their laws on how to reach these goals." [73] Furthermore, the Directive applies data protection principles to law enforcement, police, and security authorities by requesting data protection offices, 'periodic erasure of data,' data protection impact assessment, and other data protection activities.[74]

2.2.2. *Policy Regulatory Framework*

Data protection and cybersecurity efforts can be visible through the EU's policy through guidelines, recommendations, and ethical frameworks such as White Paper on Artificial Intelligence[75], Ethics Guidelines for Trustworthy AI[76], Artificial Intelligence for Europe[77], Coordinated Plan on Artificial Intelligence[78] the Proposal for a Regulation on a European approach for Artificial Intelligence[79] and other.

[72] Crider, 'Mapping Regulatory Proposals for Artificial Intelligence in Europe'.
[73] 'European Union: Regulations, Directives and Other Acts'.
[74] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[75] European Commission, 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust'.
[76] European Commission, 'Ethics Guidelines for Trustworthy Artificial Intelligence'.
[77] European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe'.
[78] European Commission. Communication from the European Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Coordinate Plan on Artificial Intelligence
[79] European Commission, Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.

Speaking of AI regulation, after its White Paper on Artificial Intelligence[80] and the leaked draft version of the Proposal[81] which showed setting strict approach to AI from the European Commission[82], the final Proposal version confirmed consistency[83] with the Charter, GDPR, and the Law Enforcement Directive, addressed additional risks of AI concerning data protection and emphasized the role of EU leadership in AI globally – especially when speaking of human rights approach.

The Proposal for a Regulation on a European approach for Artificial Intelligence is a proposal for the act for AI which would implement strict rules on high-risk AI and prohibit the use or misuse of AI that could directly endanger the safety of lives and violate fundamental rights, including systems used for manipulation of behavior of users as EU visibly prioritizes human-centered approach to AI: "the protection of people's data is especially important in the development of trustworthy artificial intelligence, a priority set in the strategy Artificial Intelligence for Europe"[84] and a key step in the path toward data-driven competition.[85] Furthermore, the Proposal is often described as a 'GDPR for AI' as it lays an essential foundation for policies and use of AI, also based on the previous guidelines for data protection laid down in GDPR:

However, the Proposal uses the term 'cybersecurity'[86] three times in total, mainly in the context of high-risk AI systems and their security: "To ensure a level of cybersecurity

[80] European Commission, 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust'.
[81] European Commission, Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.
[82] Heikkila, 'Europe Eyes Strict Rules for Artificial Intelligence'.
[83] "*Consistency is also ensured with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality. The proposal is without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems*." See: European Commission, Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.
[84] European Commission, 'Ethics Guidelines for Trustworthy Artificial Intelligence'.
[85] Ferrándiz and Degli-Esposti, 'After the GDPR'.
[86] "*High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities. The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems*

appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure." However, the Proposal also uses a privacy-preserving mechanism mainly in the context of high-risk AI systems[87], which cannot be considered as adequate data protection. Thus, it is essential to emphasize that in the first stages of AI arrival, security must be a priority from the start. Further on, the Proposal notes that in case if necessary due to ensuring bias monitoring concerning the high-risk AI systems, "the providers may process special categories of personal data (…) and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued."[88]

On the other hand, Proposal limits the use of verbs when it comes to clearly express the difference between 'may' or 'should.' It could confuse stakeholders working with big data in understanding the law-binding, mandatory element once the Proposal is laid down. Thus, why would security measures such as anonymization be mandatory just for high-risk systems? There are several unclarified points that are not fully answering the challenges approached by European Union Agency for Cybersecurity (ENISA), which was reformed through the EU Cybersecurity Act[89] that strengthens the agency and established cybersecurity certification framework for products and services. ENISA signals the need for the EU to put "cybersecurity

shall be appropriate to the relevant circumstances and the risks." In European Commission, Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.

[87] "*To the extent that it is strictly necessary for the purposes of ensuringbias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal datareferred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued*." Article 10(5) of the European Commission, Council of the European Union.

[88] Ibid.

[89] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

and data protection at the forefront,"[90] concluding that "secured AI is the foundation for any further work on AI."[91]

2.3. Implications of the Regulatory Framework on Data Protection and Cybersecurity of the Big Data

Among global AI trendsetters, it seems that the EU faces the heaviest legal implications when it comes to data protection in AI, caused by the current state of legal regulations on data protection which are not adopted for emerging technologies. Ironically, a legal framework that should primarily be considered as an asset can also pose certain limitations in the future. For example, stricter yet not completely aligned provisions of the data protection legislation with AI could harm innovation, such as GDPR, as it will "come at a significant cost in terms of innovation and productivity. EU policymakers need to recognize that a failure to amend the GDPR to reduce its impact on AI will all but consign Europe to second-tier status in the emerging algorithmic economy."[92]

However, by temporarily putting aside the challenge for the innovation limitations that might affect EU companies, one can realize that the EU regulatory framework partially extends even outside of the original EU territory through GDPR, which means that the personal information of the EU citizens will be protected in big data when it comes to AI and that GDPR provisions will affect most major companies, with the possibility to affect other global regulatory frameworks as well.

[90] European Union Agency For Cybersecurity, 'AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence'.
[91] Ibid.
[92] Wallace and Castro, 'The Impact of the EU's New Data Protection Regulation on AI'.

Previously discussed legal instruments, such as GDPR, have already left important implications that concern both law and policies globally, and it impacts all organizations inside and outside the EU which are processing the data of European citizens, thus strongly raising the standard of methods and security of collection, storage, and processing of personal data that have to achieve the same ethical and security level as the EU. GDPR recognizes security as a way to "reinforce individual rights and freedoms as a whole and enables the centrality of humans vis-à-vis machines."[93]

This Brussels effect[94] will result in a positive worldwide influence in law and policy where the EU as a normative power, hopefully, sets a global standard on data protection in AI as GDPR requires "appropriate technical and organizational measures to ensure a level of security appropriate to the risk" in Article 32[95], therefore requiring application of principles such as data encryption, physical protection of the data, pseudonymization, access control.[96] Additionally, privacy by design and by default is mandatory within GDPR, as enshrined in Article 25 of the GDPR, thus setting privacy and the security of personal information as a priority thorough all phases of system development, its routines, and in regular use – as a standard-setting.[97]

There are two forms of de-identification relevant for GDPR that apply within the EU regulatory framework, anonymization and pseudonymization, which stand as an essential setting for privacy-preserving solutions in the age of AI and protect the cybersecurity of personal information in big data. While anonymization is a process that makes the identification of the data subject in a data set almost impossible for identification,

[93] European Union Agency For Cybersecurity, 'AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence'.
[94] The Brussels effect refers to the EU's influence and power to regulate certain laws outside its borders through market mechanisms globally. See more: Bach and Newman, 'The European Regulatory State and Global Public Policy'.
[95] Article 32 of the GDPR regulates security of processing of personal data.
[96] Gruschka et al., 'Privacy Isssues and Data Protection in Big Data: A Case Study Analysis Under GDPR'.
[97] 'Report: Artificial Intelligence and Privacy'.

pseudonymization makes it almost impossible to identify the data subject without additional information that is related to the data subject.[98]

Once the data is anonymized, the dataset falls outside of the GDPR scope, and relaxed rules boost innovation. As stated in Article 2 of the GDPR, the original scope of the GDPR applies only to personal data. At the same time, Article 4 of the GDPR specifies that personal data is "any information relating to an individual or identifiable natural person"; therefore, "a simple method to conform to all requirements of GDPR is to process only anonymous data."[99] However, it is only a matter of time until when GDPR reconsiders the term 'anonymity' as there is still a possibility of successful individual re-identification even in personal data anonymization by combining the dataset with other, additional information.[100] As technology advances, it will be essential to understand how will GDPR adapt to further challenges and embrace modifications to keep up the protection in line with the technology innovation that can also affect policy regulation.

Unlike fully anonymized data and despite some relaxations of restrictions, pseudonymized data still falls under the scope of GDPR due to possible attribution of additional information that could be used to identify a natural person[101], as stated in Recital 26 as per GDPR's definition in Article 4 on pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and is subject to separate technical and organizational measures to ensure the personal data is not attributed to an identified or identifiable natural person".[102]

[98] Cavoukian and Castro, 'Big Data Nad Innovation, Setting the Record Straight: Anonymization Does Work'.
[99] Gruschka et al., *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*.
[100] Ibid.
[101] Wallace and Castro, 'The Impact of the EU's New Data Protection Regulation on AI'.
[102] Article 4 of the GDPR regulates pseudonymization.

Pseudonymization is explicitly defined as a data minimization measure under Article 5 of the GDPR – as a processing principle referred to limitation of only necessary personal data collection and processing for an as shorter time as needed. Besides protecting the personal information, the data minimization principle thus proposes a limitation on time that personal information, usually in large quantities, is being held, therefore minimizing the risk of hacking the data both by internal or external parties: "The fact that data controllers do not have sufficient incentives to apply optimal cyber-security measures most likely enhances this risk of data leakage (…) data minimization requirements can minimize this risk. [103] The progressive principle of security proportionality[104] is also applied – the higher the risk for rights and freedoms of data subjects, the more robust security protection is required.

On the other hand, a notable paucity of studies investigate how GDPR fails to adequately define big data [105]and address big data practices as it is "in incompatible with the data environment that the availability of big data generates," thus rendering many GDPR provisions, in simple words, irrelevant and seen as an obstacle "while stalling innovation in Europe and limiting utility to European citizens, while not necessarily providing such citizens with greater privacy protection."[106] In addition to this, the cost of putting security among the principles of data protection as a precondition for processing is unattractive from the economic point of view as a phenomenon[107] directly related to economic actors to "bargain risks with investments."[108] From the legal perspective, this results in a conclusion that data processing should be executed on anonymized data to avoid GDPR and possibly achieve more productive work on big data. In any other case, data processing of the EU citizens might require data

[103] Zarsky, 'Incompatbile: The GDPR in the Age of Big Data'.
[104] Article 32 of the GDPR regulates security of processing of personal data.
[105] Gruschka et al., *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*.
[106] Zarsky, 'Incompatbile: The GDPR in the Age of Big Data'.
[107] Gordon and Loeb, 'The Economics of Information Security Investment'.
[108] European Union Agency For Cybersecurity, 'AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence'.

protection impact assessment (DPIA)[109] and could cause penalties for non-compliance, such as fines up to 10 or 20 million euros or 2% to 4% of annual global turnover.

At the end of the day and despite the bureaucracy complications, both the Charter and GDPR inspired other countries and companies, GDPR being more successful as many businesses worldwide have decided to adapt to GDPR norms[110] due to collaboration with European companies and the European Union market, but also due to processing personal data of EU data subjects: "The extraterritorial reach of the GDPR is further increasing its influence, primarily through organizational practice and procedure, as corporations outside the EU realize they have to comply with the GDPR because they are processing the personal data of EU data subjects."[111] In this respect, it can be concluded that "with the GDPR and the ePrivacy Directive, the European Union has established itself as a world leader in data protection."[112], but also inspired many to follow a similar path – thus, the Brussels effect took place.

Despite setting up goals to serve as a global example, the U.S. is witnessing the rest of the world slowly adapting to GDPR or being influenced in some way by the European Union approach, "at the expense of the U.S. way which has not attained the same success."[113] Still, the U.S. participates in collaboration, discussion, and partnerships[114] with G7 and G20 countries on data protection and AI competition (i.e., OECD). It is OECD Privacy Guidelines that, as a soft instrument serving for international minimum privacy standards, started making

[109] Article 35 regulates DPIA and privacy-related impact assesment.
[110] "*The reasons for the widespread adoption of the EU model are pragmatic. The EU requires that countries wishing to do business in the EU have equivalent data protection requirements*." See: Sullivan, 'EU GDPR or APEC CBPR?'
[111] "*The reasons for the widespread adoption of the EU model are pragmatic. The EU requires that countries wishing to do business in the EU have equivalent data protection requirements*." See: Sullivan.
[112] Gruschka et al., *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*.
[113] Moschell, 'And There Was One: The Outlook for A Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection'.
114 "*On an international level, the report says the U.S. worked with the Organisation for Economic Co-operation and Development to help support "international consensus agreements on fundamental principles for the stewardship of trustworthy AI." The U.S. government also said it worked with other international partners during the G7 and G20 meetings*." See:Bracy, 'Takeaways from New White House Annual Report on AI'.

differences between the U.S. and the EU, where the EU decided to introduce more strict regulations.[115]

European Union puts a strong focus on human rights in the digital age, which is visible not just in the Charter and GDPR, but also in drafting and legislating numerous proposals to safeguard data, privacy and human rights next to emerging technologies such as the ePrivacy Directive, Data Governance Act, both law-binding and recommendation types of legislation, introducing data protection through hard and soft law. At the end of the day and despite the bureaucracy complications, both the Charter and GDPR inspired other countries and companies, GDPR being more successful as many businesses worldwide have decided to adapt to GDPR norms[116] due to collaboration with European companies and the European Union market, but also due to processing personal data of EU data subjects: "The extraterritorial reach of the GDPR is further increasing its influence, primarily through organizational practice and procedure, as corporations outside the EU realize they have to comply with the GDPR because they are processing the personal data of EU data subjects."[117] In this respect, it can be concluded that "with the GDPR and the ePrivacy Directive, the European Union has established itself as a world leader in data protection."[118], but also inspired many to follow a similar path – thus, the Brussels effect took place, which might occur again – with the AI. However, in order to successfully achieve the Brussels effect in the field of AI, a strong unity first has to exist on the supranational level of the European Union when it comes to the challenge of hard law versus soft law approach – many Member States such as Denmark, France, Finland, and Estonia are calling for a soft law approach[119] on this matter due to the fear

[115] Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?'
[116] "*The reasons for the widespread adoption of the EU model are pragmatic. The EU requires that countries wishing to do business in the EU have equivalent data protection requirements*." See: Sullivan, 'EU GDPR or APEC CBPR?'
[117] "*The reasons for the widespread adoption of the EU model are pragmatic. The EU requires that countries wishing to do business in the EU have equivalent data protection requirements*." See: Sullivan.
[118] Gruschka et al., *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*.
[119] Stolton, 'EU Nations Call for "Soft Law Solutions" in Future Artificial Intelligence Regulation'.

that overregulation will kill innovation and the private sector. In contrast, others, like Germany, disagree.[120]

To conclude the subchapter, despite not originally written for data protection and cybersecurity of big data in AI, GDPR does engage with previously mentioned challenges such as compromised privacy during data operations[121], disclosure of personal information[122], lack of data governance policies[123], lack of data protection compliance of third parties[124] and profiling of end-users[125], but further adjustments would be needed for re-identification persistent, updated methods of data pseudonymization together with additional privacy-preserving updated when it comes to security requirements of data protection in big data and enormous datasets, which can be further stressed and implemented through the policy framework.

[120] Grüll, 'Germany Calls for Tightened AI Regulation at EU Level'.
[121] "*Data manipulation or erroneous handling during Processes like Data Exploration or Pre-Processing may lead to intentional or unintentional data breaches respectively and accordingly lead to legal concerns over privacy breaches*." In ENISA European Union Agency For Cybersecurity (2020), *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence.*
[122] "*At all stages of the AI lifecycle, disclosure of personal information (either directly or by means of correlation) is a noteworthy threat. The threat is particularly manifested in the absence of verified data accuracy of sources, lack of data randomization, lack of pseudonymity mechanisms, etc.*" In ENISA European Union Agency For Cybersecurity (2020), *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence.*
[123] "*When personal data are processed, the existence of data governance policies is a part of data controller's accountability.*" In ENISA European Union Agency For Cybersecurity (2020), *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence.*
[124] "*This threat refers to the lack of compliance of the third parties with respect to applicable data protection regulations.*" In ENISA European Union Agency For Cybersecurity (2020), *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence.*
[125] "*Labeling may lend itself to a potential threat to anonymity and privacy by acting as a form of profiling.*" In ENISA European Union Agency For Cybersecurity (2020), *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence.*

CHAPTER 3. JURISDICTION OF THE UNITED STATES OF AMERICA

3.1. Cultural Values Presented in the Constitution: Positioning and Understanding The Right to Privacy

Series of human rights are protected legally on the federal level through the Constitution of the United States and its Bill of Rights, state constitutions, treaties, and through case law by establishing a judicial precedent that even can expand the scope or certain rights over the time. However, despite middle to high ranking[126] on overall protection of human rights and its multilateral ambitions to safeguard human rights globally, the United States is criticized due to the lack of complete federal protection of rights in several fields[127], including data protection and surveillance[128,129], thus resulting in the downward trend on the list.

Furthermore, additional challenges might arise at first while identifying the right to data protection within the U.S. Constitution or regulatory framework on privacy. Initially, the Bill of Rights does not contain data protection, so it has to be assumed that it is most probably classified under the right to privacy where it is not explicitly divided. However, the U.S. Constitution does not directly recognize the right to privacy either – only through further analysis of the Constitution and case law, stare decisis one can understand its integration within the Fourth Amendment that formed over time due to advancement of technology and necessary modification of law principles.

Applying constitutional principles in the digital age and age of changing technological environment, particularly the Fourth Amendment to modern technology, was shown as necessary, especially when there was no precedent to start from: "the protection granted by the

[126] 'World Report 2020'.
[127] 'US Criticised by UN for Human Rights Dailings on NSA, Guns and Drones'.
[128] Cobb, 'Data Privacy and Data Protection: US Law and Legislation'.
[129] Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?'

law must be placed upon a broader foundation."[130] Administering the Fourth Amendment in the digital age starts with the court analysis that the right has been violated if there was unreasonable search or seizure of protected things that apply in specific federal laws even[131] to communication and data as a part of requiring "fuller awareness of property and contract rights."[132]

Therefore, data protection is lined under the right to privacy which is not recognized by the Constitution but is interpreted through several amendments by the Supreme Court as a right, closely aligned to the Fourth and Fourteenth Amendment,[133] with no central federal privacy law, rather with vertically-focused privacy laws and sector-specific and consumer-oriented data protection. This can be seen as a minimalistic approach towards safeguarding privacy, primarily due to data protection laws dependence on state laws and regulations as "there is no single, comprehensive federal law regulating the collection and use of personal data,"[134] unlike the GDPR in the EU. All steps are carefully taken in order not to intentionally harm with strict data protection regulations the economy, its businesses and industries, and in some cases, even the national security, making the U.S. the space of more innovation and advancements due to fewer strings on the beneficial flow of personal data, but also fewer safeguards for human rights.

The U.S. tried to ensure free flow of data through its proposed and failed Trans-Pacific Partnership Agreement to non-EU countries to follow its lead in opposing data localization restrictions which the U.S. sees as trade barriers[135] as "there is no special requirement for

[130] Warren and Brandeis, 'The Right to Privacy'.
[131] 'Invasion of Privacy Law and Legal Definition by USLegal, Inc.'
[132] Harper, 'A Twenty-First Century Framework for Digital Privacy: Balancing Privacy and Security in the Digital Age'.
[133] 'Invasion of Privacy Law and Legal Definition by USLegal, Inc.'
[134] Jolly, 'Data Protection in the United States'.

[135] Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?'

transferring personal data from the U.S. to a third country."[136] Contrary to the spirit of such proposed collaboration, the U.S. On the other hand, the U.S. sees the importance of the protection of personal data in the context of national security as visible through its limiting acquisitions of large American controllers of personal data by foreign entities.[137]

Additionally, the U.S. legislation is quite picky regarding the type of people it protects. While the EU[138] offers a broad scope of data protection when it comes to the identity or location of individuals, it broadly protects regardless of their citizenship, while the U.S., besides applying a narrow set of entities, "limits their protection to U.S. citizens and residents."[139] Finally, there is no particular observatory board for overseeing the implementation of data protection instruments to safeguard privacy[140], but the U.S. Federal Trade Commission (FTC) has jurisdiction over privacy and data security practices.[141]

For the purpose of the comparison and the legal analysis, the critical legal instruments considered to be essential for this comparative study will be selected and analyzed: (1) Electronic Communication Privacy Act with a brief overview of the relevant Patriot Act for its importance on the federal level scope; (2) California Consumer Privacy Act for its slight resonation with the European GDPR. These legal instruments will also be briefly discussed compared to the EU legislation from the perspective of the protection of human rights.

Regarding the US policy framework relevant for data protection and cybersecurity in AI, a brief overview will be provided of (1) American AI Initiative; (2) Executive Order on Promoting the Use of Trustworthy AI in Federal Government while briefly examining (3) The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update and

[136] Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?'
[137] Pernot-Leplay.
[138] Article 4 of the GDPR regulates pseudonymization.
[139] Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?'
[140] 'DLA Piper: Data Protection Laws of the World'.
[141] Ibid.

(4) U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools. For the purpose of the detailed policy analysis, the American AI Initiative and Executive Order on Promoting the Use of Trustworthy AI in the Federal Government will be primarily consulted in the context of data protection and cybersecurity relevant to AI.

3.2. The US Regulatory Framework Through the Prism of Data Protection and Cybersecurity Relevant for AI

3.2.1. *Legal Regulatory Framework*

Created to restrict government monitoring and surveillance, the Electronic Communication Privacy Act (ECPA) covers only 'hard' telephone lines without other digital and electronic means of communication or digital data created within the communication.[142] Although Electronic Communication Privacy Act (ECPA) has been issued in 1986 on the federal level, currently, there is no other legislation alike that is covering the scope of the whole US territory at once. Together with its added Stored Communications Act[143] (SCA) that prioritizes security and sector-specific industry approach rather than data protection as a part of privacy principle, "much of ECPA is directed at law enforcement, providing 'Fourth Amendment like privacy protections' to electronic communications.

However, ECPA's three acts also contain privacy obligations relevant to non-governmental actors."[144] As a whole with its additions, ECPA stays important due to the prohibition of accessing stored communication, telephone calls or transmission of electronic data by third parties, while still not covering all types of communication, data and records –

[142] Electronic Communications Privacy Act.
[143] Stored Communications Act 18 U.S.C. Chapter 121 §§ 2701–2712.
[144] 'Report on Data Protection Law: An Overview R45631'.

and the government can still demand passing over personal consumer data from service providers being used by users[145] as ECPA covers: wire or oral communication, communication made through outdated paging device, communication caught through a tracking device and electronic funds transfer information.[146]

More disputable than ECPA regarding data protection and privacy, the surveillance-focused (anti-terrorist) USA Patriot Act, fully titled as Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism**,** was brought after the September 11 attacks (9/11) as a part of government policies to answer terrorism, therefore extending power and rights to government and authorities to oversee electronic communication: "the amendments the USA PATRIOT ACT made to those two acts, particularly as they relate to government surveillance of individuals suspected of having some connection to terrorism, significantly reduced legal protections for personal privacy."[147]

The Patriot Act seemed, unlike ECPA, to allow for security reasons what previously was hoped to be permanently forbidden or restricted, starting with increased scope and target of surveillance of both domestic and international citizen's phones, financial accounts, increased penalties for terrorism crimes, including an extended list of crimes classified under terrorism, as well as extended resources for agencies and national securities to be used in counterterrorist efforts and prevention of any kind of terrorism, which also includes border security, improved intelligence collection, etc.[148]

This empowerment of the National Security Agency has partially contributed to challenges in cross-border transfers of personal data that are affecting EU citizens who were users of American companies and social media and whose data was transferred to the U.S. in

[145] Schwartz, Mulligan, and Mondal, 'Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues'.
[146] Electronic Communications Privacy Act. § 2510
[147] Klau, 'Privacy, Security, and the Legacy of 9/11'.
[148] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act).

order to be processed. Under the Court of Justice of the European Union and rulings in Schrems I[149] and II[150], the EU has decided to abandon both the International Safe Harbour Privacy Principles and the EU-US Privacy Shield between the EU and the U.S. in order to safeguard the privacy of the EU citizens, until more detail agreement is laid down.

When it comes to positive examples of data protection close enough to the European approach, it is vital to mention Internet Privacy Protection and California Consumer Privacy Act (CCPA), often wrongly dubbed as California's GDPR[151]. Initially brought by the U.S. Federal Trade Commission, the former was voted by White House to be abolished, having this action also supported by the backers from the industry and businesses stating that, besides profit purposes, it allows "providers to use data-driven targeting could benefit consumers by leading to more relevant advertisements and innovative business models.[152]"

This leaves CCPA as the closest legislation instrument close to GDPR, which made California be the first "U.S. state with a comprehensive consumer law,"[153] despite not having the exact scope of protection like GDPR – CCPA protects only the U.S. citizens residing in California and their personal information from 'bigger'[154] businesses. Furthermore, it offers a narrow scope of data protection, purely consumer-focused with significantly lower protection than the GDPR, but it does have a multisectoral and multi-industry approach, and "several areas where the CCPA requirements are more specific than those of the GDPR or where the GDPR goes beyond the CCPA requirements."[155]

[149] Case C-498/16 Maximillian Schrems v Facebook Ireland Limited.
[150] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.
[151] Bahar, Sand, and Wilson-Bilik, 'California's GDPR Has Become Law'.
[152] Fung, 'The House Just Voted to Wipe Away the FCC's Landmark Internet Privacy Protections'.
[153] Jehl and Friel, 'CCPA and GDPR Comparison Chart | Practical Law'.

[154] "The CCPA applies to for-profit businesses that do business in California and meet any of the following: (1) Have a gross annual revenue of over $25 million; (2) Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or (3) Derive 50% or more of their annual revenue from selling California residents' personal information." See more: 'California Consumer Privacy Act (CCPA)'.

[155] Jehl and Friel, 'CCPA and GDPR Comparison Chart | Practical Law'.

By guaranteeing specific data protection to all California citizens, CCPA stands out for regulating when it comes to the (1) consent on the collection of personal information and request to know which personal information is being collected in Cal. Civ. Code § 1798.100; (2) the request to delete any personal information of the user or customer in Cal. Civ. Code § 1798.105.; (3) the right to opt-out and direct a business of selling consumer's personal information to third parties in Cal. Civ. Code § 1798.120, and other, as relevant provisions to safeguard the personal information of Californian citizens.

Cybersecurity, on the other hand, is already regulated through the collaboration between the government and private sector through Cybersecurity Act the US[156] to benefit individual rights, privacy, economic interests, and national security. The Act defines cybersecurity purpose as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." [157] Yet the regulation ambition is primarily focused on matters concerning national security and less cybersecurity of personal information.

3.2.2. *Policy Regulatory Framework*

According to the OECD.AI policy observatory database, the US has currently impressive 47 ongoing initiatives[158], together with the American AI Initiative national strategy for 'maintaining American leadership on AI' that was laid down through the Executive Order 13859[159] by the White House's Executive Office of the President on February 11, 2019, thus resulting with the National Institute of Standards and Technology in producing a plan on

[156] Feinstein, Cybersecurity Information Sharing Act.
[157] Ibid.
[158] 'OECD.AI Database of National AI Policies Powered by European Commission and OECD'.
[159] Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence.

federal engagement in AI standards. The U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools emphasized nine essential goals for the US national strategy on AI standards, including concept and terminology, data and knowledge, human interactions, metrics, networking, performance testing, and reporting methodology, safety, risk management, trustworthiness[160]. The concept of privacy and security is mentioned nine times in total, most notably in compliance with international standardization, such as OECD guidelines on ethical approaches.[161]

The White House has signed an executive order on ethical AI development.[162] Yet it is still not fully clear how will American AI Initiative or the upcoming AI regulation in the U.S. will protect and secure personal data for in the AI or AI supply chain – but the priorities are clear as there is already developed a strategy for competition and cooperation, stating: "The race to research, develop and deploy AI and associated technologies is already intensifying strategic competition (…) the U.S. government must embrace the AI competition and organize to win it.[163]

Thus, the national strategy on AI strongly emphasizes priorities related to technology and innovation development, primarily related to the private sector that includes key policies and practices such as 'unleashing AI resources,' 'removing barriers to AI innovation,' and 'promoting an international environment supportive of American AI innovation' and other.[164] On the one hand, these new regulatory principles aim to enhance innovation by easing regulatory framework while contradictory on the other hand, to protect civil liberties while the US aims for keeping the AI global leadership status.

[160] 'The U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools'.
[161] The U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools, pg. 16
[162] Lawrence, Executive Order: Supporting the development of guidelines for ethical development of artificial intelligence.

[163] 'Final Report: National Security Commission on Artificial Intelligence'.
[164] Parker, 'The American AI Initiative: The U.S. Strategy for Leadership in Artificial Intelligence'.

Executive Order on Promoting the Use of Trustworthy AI in Federal Government[165] highlights ten priorities on enhancing the trustworthiness of AI by supporting the development of selected guidelines for the ethical development of AI. Among these priorities, most relevant for the data protection and cybersecurity of the big data are 'information privacy and the protection of one's personal data' and 'safety, security, and control of AI systems now and in the future.'[166] Nevertheless, no further explanation or timeframe is given on how and when the guidelines will be further executed through more detailed policies and actions.

The clear expression of the US ambitious plans on AI development and innovation is emphasized through The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update "in order to effectively collaborate and engage with the private sector, academia, the public, and like-minded international partners."[167] Furthermore, as "advances in AI technologies have been largely driven by the American private sector,"[168] this national R&D plan prioritizes AI innovation and growth by easing regulatory 'obstacles,'[169] at the possible cost of data subjects.

The U.S. also set up a plan of 'maintaining' the global power when it comes to AI, partially mentioning its ambitious plans in the American AI initiative[170] while prioritizing innovation and business and lacking focus on data protection. Through its plans, the U.S. states that cooperation with other states, global actors, and institutions is a key to their AI plan and is an initiator and supporter of a few.

[165] Lawrence, Executive Order: Supporting the development of guidelines for ethical development of artificial intelligence.
[166] Ibid.
[167] Saslow, 'Understanding US Federal AI Policy'.
[168] Ibid.
[169] The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update.

[170] "*Recognizing the strategic importance of AI to the Nation's future economy and security, the Trump Administration established the American AI Initiative via Executive Order 13859 in February 2019*." See: Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence.

3.3. Implications of the Regulatory Framework on Data Protection and Cybersecurity of the Big Data

Unlike the EU, there are fewer legal data protection implications for upcoming policy on AI and the US regulatory framework in general as the approach of the US towards data protection and AI in general is ethical. However, a strong(er) emphasis is on boosting innovation and preserving the leadership role in the global AI race. However, there are more implications for safeguarding data protection as a human right or the level of cybersecurity of personal data in the AI supply chain. By not laying down a federal bill that would emphasize safeguarding personal information through data protection as a human right thorough States: "the absence of a centralized federal data protection regime imposes a burden of legal complexity on anyone seeking access to protected data, whether an office of law or a security manager for a commercial entity (...) that leaves many data privacy grey areas, which in turn create far too much latitude for anyone seeking to use an individual's data without notice or consent, whether for profit or protection of the nation."[171]

However, the lack of legal regulation in this field might have significantly contributed to the exponential growth of businesses, innovation, and, therefore, profit. Hence, by allowing the industry that benefits from the lack of data protection regulation, there has been the rise of the imbalance of power between users and corporations, especially digital platforms that live and profit from information gathering, and that urgently seeks for the State in the mediator role in order to provide fair practices, transparency, and ethical competition. Such platforms can also be natural monopolies, thus having the potential to reach for a power more potent than the

[171] Bignami, 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining'. In Cobb, 'Data Privacy and Data Protection: US Law and Legislation'.

national government as well as influence, which can be recognized as surveillance capitalism.[172]

How is this causing further implications for AI and AI policy? With unbalanced power, "platforms can become knowledge monopolies in certain areas, such as AI development if they decide to aggressively invest to attract all specialists in a certain domain (…) lack of civil servants with the appropriate technical skills may undermine the ability of public authorities to adequately perform their duties and strike a balance between corporations and data subject's interests."[173]

Furthermore, through the uncontrolled non-ethical approach of personal data gathering, together with the lack of federal data protection regulations that could safeguard personal information and guarantee ethical collection, storage, and processing, platforms can develop a potential tendency for manipulative actions on their users. Unlike the EU, the massive collection of data is not legally regulated on the federal level, having California as the only State as an exception, which means transcending such practices to AI-driven technology, could potentially escalate the current imbalance of the powers, thus not making any easier efforts on achieving the joint, ethical standard in the international framework that desperately needs human rights-oriented standards on data protection.

Nevertheless, it seems that the regulatory policy framework covers data protection better than the legal regulatory framework, despite lacking more details on the execution of safeguarding personal data in the age of AI and cybersecurity of big data. Unlike in most of the examined key legislations, data protection and cybersecurity are adequately addressed, despite

[172] Cobb, 'Data Privacy and Data Protection: US Law and Legislation'.
[173] Ferrándiz and Degli-Esposti, 'After the GDPR'.

lacking further explanations on safeguards. However, here we also have a contradictory setting in which the American AI Initiative encourages unleashing AI to enhance access to high-quality Federal data and easing further regulation to remove barriers to AI innovation while guaranteeing the maintenance of data privacy and security. In order to benefit innovation, the US aims to stay low when it comes to regulation of AI on the national level: "as such, it comes as no surprise that the US government's vision of its role, as a regulator, is limited (…) the US government is focused on ensuring that it does not hinder the development of AI technologies, "allowing a thousand flowers to bloom."[174]

[174] Finley, 'Obama Wants the Government to Help Develop AI'.

CHAPTER 4. JURISDICTION OF THE PEOPLE'S REPUBLIC OF CHINA

4.1. Cultural Values Presented in the Constitution: Positioning and Understanding The Right to Privacy

Probably one of the most accurate approaches that could be taken in order to understand the type and development of specific human rights and their context within the contemporary Chinese values and standings is through historical perspective with a particular focus on the correlation of duties and rights that are reflected in the current Constitution as a combination of traditional values and Western imported vales since 1840.[175]

However, China understands the concept of the rule of law differently than the West – including the concept of human rights: "For several decades in the PRC's history, human rights were regarded as a concept of the West. (…) To encourage human rights was to encourage capitalism." [176] Because of its historical experience, China has always prioritized state sovereignty and national security on the top of its national interest, ahead of human rights: "against the specific background in which China lost its sovereignty and the Chinese people were exploited by colonial powers, the concept of rights developed by the Chinese intelligentsia were different from universal principles, rather it served as an instrument – to realise the revival of China."[177] China's Constitution heavily relies on the concept of social duties but is not supreme. Neither is the law itself, which allows political actors and the

[175] Ma, Zhao, and Liao, 'The Values Demonstrated in the Constitution of the People's Republic of China'.
[176] Men, 'Between Human Rights and Sovereignty: An Examination of EU–China Political Relations'.
[177] Junru, 'Understanding Human Rights: An Issue in EU-China Relations'. In Men, 'Between Human Rights and Sovereignty: An Examination of EU–China Political Relations'.

government to bypass the Constitution[178], especially in the name of public safety and sovereignty, which are considered to be above human rights.[179]

As a socialist country, in which all nationalities of the People's Republic of China are equal according to Article 4 of the Constitution, the Constitution emphasizes collective interest through development and collective rights. Furthermore, the closest elements of the Constitution which could, in some way, be drawn as a parallel to the rights of people and people's ethical consideration in science and technology development, are the core pursuits of the Constitution presented as four values: progress, affluence, peace and safety, and harmony.[180] Thus, liberties and rights go hand in hand with duties, not to emphasize individual freedom but rather to "serve collective goals."[181] This is also why specific academic resources state that "privacy law in China is therefore not the protection of personal information per se, but rather a monopoly of the legitimate use of personal information concentrated in the state."[182] Yet, when it comes to the right to privacy in China and its primary law, it can hardly be detected from the Constitution, either directly like in the EU's constitutional treaty or indirectly through interpretation, like in the U.S. As visible through the Cybersecurity Law and 2018 Specification when it comes to data protection, China acknowledges human rights and democratic approach but "understands it differently than the EU"[183] and the West, resulting in personal information being introduced only as a 'consumer right.'[184] There are no special observatory boards monitoring violations of data protection, yet Cybersecurity Law introduces

[178] Chen, 'An Introduction to the Legal System of the People's Republic of China.'
[179] Men, 'Between Human Rights and Sovereignty: An Examination of EU–China Political Relations'.
[180] Ma, Zhao, and Liao, 'The Values Demonstrated in the Constitution of the People's Republic of China'.
[181] Ma, Zhao, and Liao.
[182] Lucero, 'Artificial Intelligence Regulation and China's Future'.
[183] Men, 'Between Human Rights and Sovereignty: An Examination of EU–China Political Relations'.
[184] "*When purchasing or using goods or receiving services, consumers enjoy the right to personal dignity, the right to have their ethnic customs respected, and enjoy the right to have their personal information protected*." See Article 4 of the Law on Protection of the Rights and Interests of Consumers, 2013 from China Law Translate.

State cybersecurity and informatization departments as key actors to monitor implementation and violations of the law and consumer's rights.[185]

Lastly, before further analysis is made, it is essential to mention how China advances in creating its own direction and approach in data protection legislation – not a long time ago, the U.S. sectoral approach 'the thing.' At the same time, today, it seems that EU's GDPR might be the approach China aims, especially when it comes to covering a multi-sectoral field and more robust protection of consumer rights, indicating China's change of the course in which it dropped U.S. properties for the EU ones.[186] Interestingly, the EU shows signs of its influence over certain aspects of China's data protection regulation, especially with the Specification, according to an expert who took part in the drafting of China's latest guidelines and which stated in 2018: "We are stricter than the U.S., but not as much as the EU,"[187] which marks positioning of China in between of the EU and the U.S and creation of data privacy – with Chinese characteristics.[188] One such key component of the data privacy regulation with Chinese characteristics is "separation between privacy from private actors and privacy from the government."[189] Furthermore, like the EU, China considers data localization seriously when it comes to transferring data abroad due to national security priority but does not apply extraterritorial scope as GDPR in the case of CSL. In addition to this, there is no national observatory board, but there are good chances that positive changes are on the way with the Personal Information Protection Law.

[185] Creemers, Triolo, and Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)'.
[186] "*China's data protection regime is further aligning with the GDPR , good news for both Chinese companies wanting to go global as well as foreign companies already GDPR-compliant.* " See more: Chow and Li, 'Podcast #23: China's First Comprehensive Personal Data Law'.
[187] Tse, 'Data Privacy Law'.
[188] Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?'
[189] Emmanuel Pernot-Lepay, "*China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?,*" Penn State Journal of Law and International Affairs (2020)

Nevertheless, China keeps holding a dual approach when it comes to data protection. In this way, it shows a unique approach to data protection which to some extent exceeds GDPR and U.S. law, and often some leave empty holes in law for keeping pace with innovation and time, but also for political manipulation. More examples are to be highlighted in the further analysis of individual legal instruments and policies. Furthermore, the key Chinese legal instruments closest to regulating data protection in China that will be relevant for artificial intelligence and therefore analyzed in the paper are the previously mentioned law-binding Cybersecurity Law of the People's Republic of China (CSL) and the non-binding Information Security Technology – Personal Information Security Specification (GB/T 35273-2017) with a brief overview of the upcoming Personal Information Protection Law[190] that will serve as an important basis for further AI regulation.

From the policy perspective, three national plans and guidelines are selected for further paper analysis due to their impact in the context of data protection and big data cybersecurity: (1) New Generation Artificial Intelligence Development Plan (AIDP); (2) Made in China 2025; (3) Artificial Intelligence Standardization White Paper 2018; (4) Cybersecurity Standard Practice Guide: Guidelines for Artificial Intelligence Ethical Security Risk Prevention

4.2. China Regulatory Framework Through the Prism of Data Protection and Cybersecurity Relevant for AI

4.2.1. *Legal Regulatory Framework*

China's law-binding Cybersecurity Law of the People's Republic of China (CSL) primarily introduces cybersecurity provisions, network information security, monitoring, and

[190] Qi et al., 'China Releases Draft Personal Information Protection Law'.

legal responsibility with clearly defined fines in case of a law violation. It also introduces obligations, brief instructions for secure handling of personal information and security measures for network operators operating and processing personal information in Article 41 on the collection and use of personal information and Article 42 on not disclosing or destroying personal information, while Article 44 introduces prohibition of stealing or using illegal methods to acquire personal information.[191] In addition, chapter 7 introduces the definition of personal information within the supplementary provisions, where personal information: "refers to all kinds of information (…) that taken alone or together with other information, is sufficient to identify a natural person's identity (…),"[192] similarly to GDPR.

Like the U.S., China was following the path of multi-sectoral and sector-specific data protection. However, changes are introduced with the Cybersecurity Law where more significant data protection is introduced together with the cybersecurity requirements, hand in hand with the vision of China that public safety and security is a priority, above human rights[193]. CSL introduced strict regulations for consumer-businesses, companies and corporations, in some aspects reaching even further than the GDPR [194] while extending powers to the government for data collection in order to protect and maintain public safety: "China's system is the difference between the strengthening of protection against private entities and the parallel increase of government's access to personal data, as there is still no significant privacy protection against government intrusion."[195] That clearly differs from the EU's approach that tends to protect personal data both from the business but also government sides.

[191] Creemers, Triolo, and Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)'.
[192] Ibid.
[193] „*In 2015 the National Security Law and Anti-Terrorism Law allowed the government to collect any information for the sake of public welfare and national security*." See: Sacks, 'China's Emerging Data Privacy System and GDPR'.
[194] Ibid.
[195] Li, Bronfman, and Zhou, 'Saving Face: Unfolding the Screen of Chinese Privacy Law'.

Moreover, one of the main slippery points in the Chinese laws perceived as a danger to efficient data protection is in China's approach to law – its generality and vagueness:" The law constraints many dispositions and definitions where the lack of precision gives rise to questions placing entities in a state of legal uncertainty,"[196] including law-binding CSL that, unlike non-binding Specification 2018, has imprecise language and lacks a broad scope of definitions together with further instructions on personal information and data protection. Imprecision in law, therefore, allows certain judicial and political actors to interpret it more efficiently in a direction closer to what is considered to be the best for public safety and order.

The non-binding Information Security Technology – Personal Information Security Specification ("the Specification") could be seen as an example of good practice when it comes to guidelines on the protection of personal information. It was issued by the Standardization Administration of China in 2017 and came into effect in 2018 where even as a non-mandatory and non-binding regulation, it carries "a key implementing role concerning China's Cybersecurity Law in respect of protecting personal information in China"[197] in the context of the collection of personal data of employees or third parties, therefore mostly related to business operations. China has put a strong emphasis on laws to prevent emerging technologies from misusing personal data, as can be furthermore detected in the non-binding 2018 Specification that is the closest document to the EU approach on data protection. It provides clear guidelines and comprehensive guidance for data protection, and it highly resonates with elements of the EU standards, including a broad range of definitions, showing that there is a good base to start from when it comes to creating appropriate law-binding data protection other than the Cybersecurity Law. The Specification defines its scope as "the principles and security requirements for the processing activities of collection, preservation, use, sharing, transfer,

[196] Cao, *Chinese Law: A Language Perspective*; Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?'
[197] 'Personal Information Security Specification Commentary'.

public disclosure of personal information[198] applicable to regulate processing activities in organizations, management, regulatory authorities, and agencies, therefore bringing more guidelines for the protection of consumer rights. Furthermore, the Specification introduces differences in prior consent from individuals in collection of directly collected personal information, indirectly collected personal information and collected sensitive personal information with exceptions where the Specification allows collection of personal information without prior consent directly related to national security interests, public interest.

Similarly to the EU, China also took an effort to introduce emerging technologies and digital threats to personal information by adding additional protection through articles of the Specification, serving as a potential base for the creation of an ethical AI regulatory framework in China[199], such as automatic-decision making and the right to appeal to the personal data subject in provision 7.10.,[200] helpful for setting up a more substantial base for AI regulation.

4.2.2. *Policy Regulatory Framework*

China holds an advanced position when it comes to positioning cybersecurity in big data and AI, having CSL on which further policy and legal framework can be built, thus improved with the upcoming Personal Information Protection Law that will shift data protection closer to the European approach while keeping certain Chinese regulatory specifications, as briefly discussed in the previous chapter. Furthermore, when it comes to policy regulation relevant for data protection and big data cybersecurity in the age of AI, China has published several important policy documents such as the New Generation Artificial

[198] Section 1 of the Information Security Technology – Personal Information Security Specification (GB/T 35273-2017).
[199] Wagner, 'China's Cybersecurity Law: What You Need to Know'.
[200] Section 7.10 of the Information Security Technology – Personal Information Security Specification (GB/T 35273-2017).

Intelligence Development Plan (AIDP), Made in China 2025, and Artificial Intelligence Standardization White Paper 2018, among several other national-level policy documents.

Observing globally, China had an early and strong start when it comes to AI development from a policy perspective, with a conscious effort to become a global leader in AI. Already in 2015, China published a 10-year plan of development plan to focus on becoming a technology-powered force and high-tech leading manufacturer in the form of Made in China 2025 national plan that included AI as a vital part of innovation, industry, and economic growth. By being the "first national-level legislative effort that focuses explicitly on the development of AI as a unified strategy"[201] the New Generation Artificial Intelligence Development Plan (AIDP), China set out ambitious goals on becoming a global leader in AI by 2030, the trendsetter in defining ethical norms, and on AI monetization, thus setting up directions for geopolitical, legal and ethical, and fiscal development.[202] The approach taken by China, besides economy and industry orientation, also focuses to "strengthen research on legal, ethical, and social issues related to AI, and establish laws, regulations and ethical frameworks to ensure the healthy development of AI"[203] thus indirectly improving public and national security as one of the ultimate goals of AI policies in China.[204,205]

Artificial Intelligence Standardization White Paper from 2019 is produced by the Big Data Security Standards Special Working Group of the National Information Security Standardization Technical Committee with institutional support from leading organizations in China in order to "promote the healthy, rapid, safe, and orderly development and expansion of AI technology applications."[206] While the paper explained the importance of AI industry

[201] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[202] Ibid.
[203] New Generation Artificial Intelligence Development Plan.
[204] Ruan, *When the Winner Takes It All: Big Data in China and the Battle for Privacy*.
[205] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[206] Artificial Intelligence Security Standardization White Paper (2019 Edition).

commercialization to play a positive role in accelerating innovation, industry, and information use efficiency[207], it also tackled big data security threats, risks, and challenges on big data summarized through the standardization progress overview of national and international regulations.[208]

Lastly, the Cybersecurity Standard Practice Guide: Guidelines for Artificial Intelligence Ethical Security Risk Prevention is the latest critical edition to China policy framework relevant for highlighting ethical security risks when it comes to AI. Despite its non-binding status, the Guide provides crucial directions for safeguarding ethical security of possible risks, including "respect and protection of basic individual rights and the development of management systems and mechanisms for the construction of security risk management to realize open collaboration and shared responsibility."[209] Furthermore, the Guide emphasizes several ethical security risks in Section 3., among which is also the risk of infringement of the fundamental human rights, including personal privacy, and proposes measures for risk prevention under Section 4. by stating that the basic rights of individuals, including personal privacy and property rights with special attention to the protection of socially vulnerable groups.[210] It is also essential to highlight the R&D Section 4.2. that states how no research or development of the AI that aims to harm people's basic rights should be conducted.[211]

[207] 'Global Artificial Intelligence Industry Whitepaper'.
[208] Artificial Intelligence Security Standardization White Paper (2019 Edition).
[209] 'China: TC260 Releases Cybersecurity Practice Guide on AI Ethical Security Risk Prevention'.
[210] 'China: TC260 Releases Cybersecurity Practice Guide on AI Ethical Security Risk Prevention'.
[211] Ibid.

4.3. Implications of the Regulatory Framework on Data Protection and Cybersecurity of the Big Data

After the brief analysis of legal and policy regulatory framework relevant for data protection and big data cybersecurity in the age of AI, four implications concerning further development for the AI regulatory framework have stood out: the state-centric regulation[212] of privacy targeting primarily corporations to safeguard 'consumer rights,' [213] possible implications for the AI-enabled governance through Social Credit System[214] and China's plan on becoming the driving force behind the AI ethics on the global level, concluding with soft law versus hard law impact of regulations.[215]

Among global AI trendsetters, China has put the most impressive focus on big data and understanding that big data security challenges are directly liked to AI development and has emphasized its efforts through its regulatory policy framework and national development plans on AI. It seems that even equally, or even more as innovation and industry, China prioritizes public and national security, thus producing a large number of regulations concerning cybersecurity elements, more than the EU and the US. In addition to this, China has an impressive way of integrating big data and cybersecurity in most of the examined regulations in this paper, thus exceeding the EU and the US when it comes to the integration of big data cybersecurity within the regulatory framework. Possible explanations lie behind the fact that China produces an enormous amount of data every second due to its large population and due to its strong focus on national security.

[212] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[213] Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?'
[214] Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[215] Ibid.

Regardless of stronger regulation on data protection than the US, unlike the EU, China focuses primarily on protecting 'consumer rights.' In other words, most of the previously presented regulations focus on regulating data protection and privacy between users or consumers and businesses or corporations with none or very little provided regulation for the government: "it is these large loopholes that are most revealing of China's data policy (…) it may be argued that some broad consumer protections are present, but actually this is not extended to the government."[216] Furthermore, due to the generality and vagueness of the Chinese law[217], the decisions on respecting the strength of privacy and violations would depend on the government's decisions instead of 'legal and practical constraints.[218] This whole approach of safeguarding 'consumer rights' through the current legal framework by focusing data protection safeguards primarily in the private sector slightly clash in an interesting way with current AI policy plans on development in which the government promises to ease regulatory framework for the private sector in order to "forcefully develop smart enterprises"[219] and boost innovation, like in the US.

Furthermore, despite being named as 'Asia's surprise leader on data protection[220] due to a number of regulations passed concerning privacy, data protection, and cybersecurity, China is facing backlashes on its Social Credit System, mostly on the international level. Planned as a tool to "address China's pressing social problems,"[221] the system "did not just aim to regulate financial and corporate actions of business and citizens, but also the social behavior of individuals."[222] Noting that China strives towards becoming a level trendsetter in defining

[216] Laskai, 'China Is Having an Unexpected Privacy Awakening'. In Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[217] Cao, *Chinese Law: A Language Perspective*.
[218] In Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[219] New Generation Artificial Intelligence Development Plan.
[220] Lucas, 'China's Artificial Intelligence Ambitions Hit Hurdles'. In Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[221] Chorzempa, Triolo, and Sacks, 'China's Social Credit System'. In Roberts et al., 'The Chinese Approach to Artificial Intelligence'.
[222] 'Outline for the Establishment of a Social Credit System'. In Roberts et al., 'The Chinese Approach to Artificial Intelligence'.

ethical norms on the global level as "China will actively participate in the global governance of AI, strengthen the study of major international common problems such as robot alienation and safety supervision, deepen international cooperation on AI laws and regulations, international rules and so on, and jointly cope with global challenges,"[223] such approach with strong elements of cultural relativism resulted with global counteractions, as visible in the creation of Global Partnership on AI (GPAI), further explored in Chapter 5.

Despite ambitious national plans which are positioning AI as the key priority for China's development and global position, privacy continues to be the weak point that needs further development in order to ensure data protection as a human right.

> "*China has announced to the world that it intends to become the global leader in artificial intelligence, both in terms of developing and deploying technology as well as governing it with appropriate laws and regulations. (…) As AI law continues to develop, it will likely follow a similar pattern of developing a monopoly on the legitimate use of AI as defined by the state*."[224]

Fortunately, one of the most legislation pieces in drafting that will touch data protection in the AI regulatory framework is previously mentioned Personal Information Protection Law[225] which is currently available as a draft that touches upon data anonymization and overseeing to protect cross-border data transfer, which can be considered as a significant step towards positive change. Together with the Personal Information Protection Law, CSL also serves as a basis for setting up AI regulation when it comes to data protection and already

[223] New Generation Artificial Intelligence Development Plan.
[224] Lucero, 'Artificial Intelligence Regulation and China's Future'.
[225] Qi et al., 'China Releases Draft Personal Information Protection Law'.

making a contribution to drafts supported by the Chinese Ministry of Science and Technology as well as the new National New Generation AI Governance Expert Committee.[226]

Lastly, regulatory implications regarding soft law and hard law will impact the future of AI regulation as well. It seems that some of the most progressive and advanced currents passed legislation are those which are non-binding, such as the non-binding 2018 Personal Information Security Specification and Cybersecurity Standard Practice Guide: Guidelines for Artificial Intelligence Ethical Security Risk Prevention (as the proposed Personal Information Protection Law is still a draft when it comes to legal, regulatory framework on data protection). However, despite its formally non-binding status, these legislations can still shape and impact the regulatory framework and contribute to the further ethical development of legislation.[227] This is important as, for example, the Cybersecurity Standard Practice Guide: Guidelines for Artificial Intelligence Ethical Security Risk Prevention emphasizes within the security risks that basic rights also include the right to personal privacy "that should be respected and protected."[228], thus marking an important statement and a precedent for further development of the right to privacy in the age of AI.

[226] Gal, 'China's Approach to AI Ethics'.
[227] Bird, 'China "Standardises" AI Ethics'.
[228] New Generation Artificial Intelligence Development Plan.

PART II. GLOBAL CHALLENGES IN THE NEED FOR A GLOBAL SOLLUTION FOR DATA PROTECTION AND CYBERSECURITY: THE POSSIBILITY FOR THE GLOBAL AI GOVERNANCE?

There are several definitions of global governance, from "the management of global processes in the absence of global government"[229] to "totality of institutions, policies, norms, procedures and initiatives through which States and their citizens try to bring more predictability, stability, and order to their responses to transnational challenges."[230]

For the purpose of this thesis, I have identified three types of structures of global governance relevant for artificial intelligence in the context of privacy and security matters, such as data protection and big data cybersecurity: (1) international governmental organizations (IGOs); (2) intergovernmental forums and groups; (3) international multistakeholder initiatives which I will further examine in this chapter, as well as their strengths and weaknesses when it comes to implementing ethical global AI agenda.

This part of the thesis also examines the peace and collaboration-strengthening approach supported by most international AI initiatives versus national and arms race-oriented. This is important as often easing necessary regulations to boost innovation and position in the AI arms race comes with a price for human rights, data protection, and cybersecurity of big data. In my humble opinion, global ethical governance on AI should be about encouraging very much-needed regulations to safeguard human rights as well as the collective direction of efforts from a warfare-oriented approach towards innovation and a sustainability-oriented approach to achieve, i.e., sustainable development goals. Overall, global ethical governance should also be about not easing regulations just because of the data arms race that will heavily impact data protection safeguards: "users are the biggest potential losers in this race, with their rights to

[229] Riazati, 'A Closer Look: Professor Seeks Stronger UN'.
[230] 'Global Governance and Global Rules for Development in the Post-2015 Era', 201.

privacy and personal data protection held up as a challenge to innovation."[231] Nevertheless, it is not an easy task for any international organization or initiative, bearing in mind that even though the main repeating ethical principles do not mutually exclude each other, "any global governance regime will face massive obstacles, especially for AI as it is the kind of technology that naturally resists structures and structures."[232]

[231]Creemers, Triolo, and Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)'.
[232] Medhora, 'AI & Global Governance'.

CHAPTER 5. INTERNATIONAL REGULATORY FRAMEWORKS AND TREATIES: AN OPPORTUNITY FOR CREATING ETHICAL STANDARD OF DATA PROTECTION OR FLEXING NORMATIVE POWERS?

5.1. International Structures of Partnerships and Global Initiatives on AI

OECD.AI database identifies over 600 AI policy initiatives in over 60 countries,[233] disclosing a strong tendency on moving towards localization instead of globalization when it comes to AI regulation, possibly "for the benefit of more local initiatives." [234] Despite international efforts and international cooperation structures to create a universal approach towards AI to safeguard human-centric approach towards AI, country governments, corporations, and civil society structures are producing their own sets of recommendations, principles, and guidelines.[235] Countries choose different approaches to AI regulation depending on their political, economic, and cultural values.

However, separate development and different approaches towards "the development of regulatory frameworks and guidelines does not exclude similarities between the proposals."[236] Interestingly, proposals coming from G20 countries are recurring regulatory schemes on six topics that also include privacy and safety/security concerns.[237] Furthermore, an analysis of 21 major ethical and influential guidelines (government, industry, science) published between 2016 and 2019 reveals repeated issues that are being covered, with privacy protection as the major concern, is most represented, while safety and cybersecurity were the fifths among 22 selected ethical aspects.[238] There is a number of studies examining the similarity of patterns within global and national initiatives that focus on safeguarding the human-centric approach in

[233] 'OECD.AI Database of National AI Policies Powered by European Commission and OECD'.
[234]Giardino, 'The Mirage of a Global Framework for AI Governance'.
[235] Ibid.
[236] Giardino, 'The Mirage of a Global Framework for AI Governance'.
[237] Giardino.
[238] Hagendorff, 'The Ethics of AI Ethics: An Evaluation of Guidelines'.

AI, thus creating a solid basis for starting serious conversations on global AI governance. Additionally, this paper humbly contributes to this thought. It examines similarities within the legal and policy regulatory framework of the three most influential jurisdictions for AI and their international involvement and efforts on global AI initiatives further explored through chapter 5.

5.1.1. *International Governmental Organizations*

All eyes are pointed at United Nations when it comes to the 'responsibility' of taking the first steps to shape the directions of AI and proposing guidelines for human-centred AI. The basis is already there – privacy is safeguarded in Article 12 of the Universal Declaration on Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Although it can be widely discussed how successful the implementation and normative influence of the UN legislation is, it is important to understand that "though the UDHR is often violated, it creates an aspirational global standard (..) it acts as a guide to draft national and sub-national legislation, as a framework to assess (and sometimes "name and shame") its application, and ultimately, as with the International Court of Justice, to penalize its violation."[239] Therefore, it is crucial that the UN takes these first and important steps, and they are slowly realizing, through the prism of UNESCO.

UNESCO's Ad Hoc Expert Group (AHEG) has issued the First Draft of the Recommendation on the Ethics of Artificial Intelligence[240]. The Recommendation provides recommendations on several ethical principles, including safety and security (cybersecurity)

[239] Medhora, 'AI & Global Governance'.
[240] 'First Draft of the Recommendation on the Ethics of Artificial Intelligence'.

and privacy within Section 2. Interestingly, the safety and security principle, besides focusing on ensuring safety and security throughout the lifecycle of AI systems, emphasizes that "safe and secure AI will be enabled by the development of sustainable, privacy-protective data access frameworks that foster better training of AI models utilizing quality data,"[241] thus placing a focus on the importance of quality data utilization and privacy-protective frameworks.

The Recommendation highlights privacy as a "right essential to protecting human dignity, human autonomy, and human agency"[242] that must be safeguarded throughout the AI lifecycle, both individually or collectively. Furthermore, the Recommendation stresses the importance of establishing adequate data protection frameworks and governance mechanisms either by regulatory agencies at national or supranational levels that are as well protected by judicial systems. It is essential to mention that the Recommendation also understands the importance of applying innovative privacy-preserving approaches through privacy by design approach. Despite its non-binding nature, several policy actions are proposed with recommendations for the Member States to take action, and this matter for all explored jurisdictions in the paper, the EU, the US, and China.

Despite not having China as its member, the Organisation for Economic Co-operation and Development (OECD) is important for several decisions and recommendations regarding safeguarding human rights, including privacy and data protection. The OECD is vital for its non-binding Recommendations of the Council on AI[243] that defines directions and obligations of achieving trustworthy AI by also emphasizing the importance of security and safety, directly related to data protection and cybersecurity of big data. Previously mentioned OECD.AI Policy

[241] 'First Draft of the Recommendation on the Ethics of Artificial Intelligence'.
[242] 'First Draft of the Recommendation on the Ethics of Artificial Intelligence'.
[243] 'Recommendation of the Council on Artificial Intelligence OECD/LEGAL/0449'.

Observatory[244] collects and informs on policy initiatives globally, thus providing an overview of the gravity, scope, and multicultural aspect important for further global governance development.

Council of Europe (CoE) counts neither the US nor China as its members, yet all EU Member States are also members of CoE, thus have to follow the legally binding European Convention on Human Rights and respond to the European Court of Human Rights (ECHR) in case of ECHR violations. ECHR is essential for understanding data protection and recognizing it under the right to privacy as a human right, hence further influencing the protection of privacy in legislation relevant to AI. CoE's Ad Hoc Committee on AI (CAHAI) has published recommendations for the regulation of AI in order to safeguard human rights while developing AI titled "Unboxing AI: 10 Steps to Protect Human Rights" [245] . As expected, the Recommendation fully aligns with ECHR, thus listing data protection and privacy under the 7th principle to encourage safeguarding privacy.

Despite not being directly aligned and connected to AI, CoE's legally binding Convention on Cybercrime[246] might come handy when it comes to certain aspects of data protection, partially and indirectly safeguarded through, for example, Article 19 on search and seizure of stored computer data or Article 20 on the real-time collection of traffic data.

[244] 'OECD.AI Database of National AI Policies Powered by European Commission and OECD'.
[245] 'Unboxing AI: 10 Steps to Protect Human Rights'.
[246] Convention on Cybercrime.

5.1.2. *Intergovernmental Forums and Groups*

G7 and G20 groups collect leaders of selected countries over the world significant for their economic, trade, and similar powers. Due to its importance, the topic of AI could not surpass these intergovernmental forums: "the recent G7 statement on artificial intelligence serves as a good starting point for a more global discussion on the ethos that we want driving transformative technologies in general and AI in particular"[247], enshrined in the G7's Charlevoix Common Vision for the Future of AI. While G7 includes the US and the EU as its members, G20 is the one including China as well. Therefore, the G20 meeting might be of greater importance when it comes to laying partnerships on AI between the EU, the US, and China. G20 AI principles are outlined in the G20 Ministerial Statement on Trade and Digital Economy that is supposed to, among other human-centered AI goals, "to provide a universal framework of values, principles, and actions to guide States in the formulation of their legislation, policies or other instruments regarding AI."[248] The Statement includes Annex with non-binding G20 AI Principles where human-centered values and fairness are wanted and that AI actors should "respect the rule of law, human rights, and democratic values, throughout the AI system lifecycle (…) these include freedom, dignity, and autonomy, privacy and data protection."[249] As visible, G20 AI Principles rely on the OECD Recommendation on AI and encourage Member States to follow existing frameworks aiming to safeguard human rights in AI.

[247] Medhora, 'AI & Global Governance'.
[248] 'Ministerial Statement on Trade and Digital Economy'.
[249] Ministerial Statement on Trade and Digital Economy'.

5.1.3. *International Multistakeholder Initiatives*

The first and most known is the Global Partnership on AI (GPAI) which has been founded on June 15 in 2020, and established as "an international and multistakeholder initiative to guide the responsible development and use of artificial intelligence consistent with human rights, fundamental freedoms, and shared democratic values, as reflected in the OECD Recommendations on AI."[250] Founding members of GPAI include G7 countries with 13 or more members, including the European Union (EU) with OECD as a hosting secretariat and UNESCO as an observer in the partnership. GPAI's Working Groups have already contributed a significant number of reports and findings and operate within OECD Recommendations on AI, building upon the policy framework further for the ethical AI and global AI governance. Although founding GPAI was mostly welcomed globally, what is missing from the website is the fact that the initiative started on the call of France and Canada to other G7 countries for starting the initiative which could set rules for AI – and while the U.S. avoided joining at first due to fear of overregulation which could harm innovation, they joined in establishing GPAI to counter China's AI threat and 'Orwellian surveillance apparatus'.[251] Thus, this makes GPAI at least in some way politically empowered in a way that specific goals might go directly and firmly against the policy of another non-member country, making global agreement harder to happen. The next chapter will explore this topic further.

Unlike GPAI, the International Alliance for a Human-Centric Approach to Artificial Intelligence (IA-AI) is in its early stage in 2021, launched by the EU mainly for preserving human rights in the center of AI development, innovation, policy, and law-making and open

[250] 'GPAI Frequently Asked Questions'.
[251] Banarjee, 'Can Global Alliance Stop China Becoming Artificial Intelligence Superpower?'.

for the EU bodies, governmental stakeholder, but also in some cases for EU and non-EU companies working on AI and individual experts. There is certainly a political interest, too, as the EU has to keep its status as a normative power, and therefore it will "undertake a unified approach on AI also internationally"[252] in order to preserve itself as a front-runner in global AI ethical and legal framework. Still, the EU preserves its tradition in foreign policy to keep human rights above everything, which makes this coalition fully human rights-focused.

Lastly, more business and economic focused is the latest World Economic Forum global initiative on AI named Global AI Action Alliance (GAIA) launched in 2021 that aims for achieving inclusive, transparent, and trusted AI while unlocking new economic value. With stakeholders primarily based on top companies, organizations with governments, and academics, further research will be done on designing and accelerating "the development and adoption of tools globally and in industry sectors."[253]

5.2. The Challenges of Transnational Lawmaking Affecting Safeguarding Privacy and Security of AI: Implications of the Prioritization of Geopolitical Interests

The pressure is natural when speaking of the global AI competition in different fields – from a number of conducted research on AI, businesses to laid down policies and laws. Even in coalitions aiming for global governance, tensions can be felt, while cultural and political barriers between the West and the East could seem unsolvable – it can be challenging when one out of three central AI powers of the AI race have a significantly different approach to the

[252] 'Action Document for an International Alliance for a Human-Centric Approach to Artificial Intelligence (Annex 4)'.
[253] Tedeneke, 'World Economic Forum Launches New Global Initiative to Advance the Promise of Responsible Artificial Intelligence'.

understanding of human rights such as *e.g.,* China: "For several decades in the PRC's history, human rights were regarded as a concept of the west. (…) To encourage human rights was to encourage capitalism."[254]

Additionally, China also announced to the world that it intends to become the global leader in artificial intelligence, both in technology, policy- and law-making,[255] while the U.S. concluded that "the U.S. government must embrace the AI competition and organize to win it."[256] The decisive clash of nationalism vs. globalism[257] approach on the AI challenges, which can be assessed only by joint multilateral efforts, is no good news. Thus, GPAI political background of 'western countries' with 'western values' could highly provoke if the dialogue is not set up with the rest of AI and cyber powers – even if *e.g.,* China does not fully approve approaches dictated by GPAI, communication is the key to prevention of possible conflict escalations and the key for possible collaborations in the future – maybe even on the global AI governance.

On the other hand, other initiatives might be more successful when aligning values that connect the EU, the US, and China, as visible in the examples of intergovernmental organizations and forums that are already slowly and carefully entering the soft law approach.

[254] Men, 'Between Human Rights and Sovereignty: An Examination of EU–China Political Relations'.
[255] Lucero, 'Artificial Intelligence Regulation and China's Future'.
[256] 'Final Report: National Security Commission on Artificial Intelligence'.
[257] Harari, 'Nationalism vs. Globalism: The New Political Divide'.

CONCLUSION

Innovations and next-generation technology are emerging almost exponentially, affecting the daily lives of billions of people in all parts of the world of the digital age. The most important race of the first part of the 21st century has already begun – the competition for artificial intelligence development is impacting transnational relations, business, policies, and human rights, tightening relations between the U.S. and China that dictate the pace of AI leadership through less regulated settings to benefit innovation. At the same time, European Union carefully seeks ethical governance on advanced technologies in order to prevent possible human rights violations, such as the right to data protection. However, pressured to keep on track with the ambitious competitors from the West and East, the EU does not want to miss the AI race with the US and China.

The aim of this paper was to answer the research question and its sub-questions in order to identify and understand similarities in the patterns of the EU, the US, and China legal and regulatory policy framework in the context of data protection and cybersecurity relevant for AI on which basis an ethical global AI agenda could be built on. Furthermore, the paper also provided an overview of the interconnection between data protection, cybersecurity, and global initiatives on AI and its importance for potential global governance on AI. Each of the selected jurisdictions was individually analyzed through its legal and policy regulatory framework, cultural values, and understanding of privacy through its primary law (the Charter/Bill of Rights/Constitution) and afterward mutually compared to understand if certain jurisdictions prioritize human rights, industry or national security as a primary goal achieved through the legislation and later on, through policies. By comparing highlighted findings on specific jurisdiction characteristics when it comes to defining data protection through the right to privacy as well as safeguarding data protection and cybersecurity of big data, I was able to

define three different approaches of each jurisdiction, but also similarities in the patterns which was later confirmed in selected examined AI global initiatives and that signed human-centric oriented AI non-binding documents by all three jurisdictions. Moreover, by additionally consulting scholarly papers and previously completed researches on the reoccurrence of ethical principles in AI policies and guidelines, I was able to detect the same pattern with the EU, the US, and China – despite differences in prioritization of human rights, industry or national security and in spite of different understandings of the right to privacy and approaches to data protection and cybersecurity of AI, there is a will, a plan, and a power to more or less act on these issues.

Starting with the European Union – the legal analysis that covered a brief examination of the Charter revealed it is a part of the constitutional basis of the European Union that has legally binding power in safeguarding political, social, and economic rights within the EU, including the data protection as a recognized human right, thus revealing an advanced recognition and protection of 'modern' human rights of the next generation. In other words, the EU puts human rights at the core heart of its identity and external relations, often serving as an example of an ethical leader worldwide. As the Charter reflects cultural values of the European Union, it provided a strong direction for further safeguards and development of data protection in further examined legal instruments like GDPR that represents a groundbreaking regulation on personal information and data protection with the high scope and level of protection and a special observatory board that oversees GDPR implementation. As expected in the policy analysis, the common point of all published AI policy documents is the focus on developing a human-centric AI as the highest priority as well as international cooperation that could boost ethical AI development, while detected weaknesses include possible

overregulation or slow-moving innovation and the lack of privacy-preserving challenges awareness that could have been more presented in the form of increased big data cybersecurity awareness, guidelines, and plans. Furthermore, the EU is an excellent example when it comes to lawmaking and policymaking on the supranational level that is having wide jurisdiction and therefore impacts on the EU Member States. To conclude, the EU primarily strives towards achieving ethical plans yet lacks more economical and technical initiatives as well as business models that can align economic needs and interests with people's values and standings on human rights. Through the Brussels effect, it successfully 'exports' prioritization of human rights, including the right to privacy and data protection, yet has to expand its horizon to the 'money game'. By becoming an example that can both protect human rights at the highest level and still profit from the AI innovation monetization, it would create an even more substantial effect that would resonate globally, not just through normative influence but through leading with an example. Until then, as the global AI race goes on, the EU is left behind ambitious China and the U.S. when it comes to innovation and business progress, but it is a clear winner in the race for the ethical approach to technology in order to preserve human rights and the world we know, from time to time influencing global actors as a normative power and achieving Brussels effect.

In the case of the United States of America, the Bill of Rights protects the right the privacy, including data protection through judicial interpretation of the Fourth Amendment, yet without any 'modern' and harmonized regulation like GDPR on the federal level to safeguard personal information protection and security and without special observatory boards on data protection. However, this did not prevent the US from passing legally binding legislation like the USA Patriot Act on overseeing electronic communication for security reasons to overpower previously laid down ECPA on government monitoring and surveillance restrictions in electronic communication and digital data. The only GDPR-alike legislation is CCPA that

generally protects consumer's data within California and California's citizens only. Thus, relevant legislations related to data protection can be divided into the categories of national security and consumer protection, while the AI policies are following similar dynamic – AI innovation for internal goals and AI arms race for external, all in order to maintain the AI leadership globally. To conclude, the US would have to consider tighter control on data protection in the age of AI primarily due to the fact that AI lives on big data, especially when taking into account that the US is willing to ease regulations in order to boost AI innovation led by the private sector. While the interest of the individual data protection is not satisfying, the situation is better when it comes to the cybersecurity of AI – being set as one of the important priorities in the AI; it still lacks details on the execution of safeguarding personal data in the age of AI and cybersecurity of the big data. All in all, the US has a strong, champion-based AI framework that will benefit innovation but will have to face and implement certain human-centric AI approaches coming from the international frameworks.

Lastly, the People's Republic of China has strong cultural values on collectivity and sovereignty emphasized through its Constitution, which prioritizes national security, progress, as well as harmony, with no specific directions and guidance for data protection. However, personal data protection is primarily introduced as a consumer right where corporations and businesses are obliged to follow additional regulations, while the government keeps almost unrestricted access in order to maintain public interests, national security, and harmony. Additionally, China has put impressive efforts when it comes to cybersecurity awareness, resulting in a law-binding CSL which can also be seen as an important step for further AI policy and guidelines, taking into account that among all global powers, China has enormous resources of data that has to be protected and handled securely. Additional non-binding legislation on data protection and personal information is introduced, yet with non-binding properties, that takes us to the conclusion that all security-related legislations are law-binding,

while legislation directed to protect personal data, even if more concise in some segments than GDPR, are still challenged with the non-binding status and no special observatory boards on data protection. To conclude, it is important to highlight China's cultural understandings on human rights that have to be seen through the prism of China's history and culture in order to be able to negotiate any kind of successful global governance: "as an important member of international society, China recognizes the value of human rights and democracy but understands it differently than the EU."[258] However, this should not be an excuse for not directly acknowledging data protection rights within the law-binding regulatory framework. Furthermore, the world can look upon China's developed specifications on big data, legal and policy awareness, and implementation of big data cybersecurity in the age of AI and laid down standardization documents that ensure technology security and quality, as it aims to ensure global leadership in AI.

When it comes to global governance on AI possibilities based on the identification of similar patterns within the jurisdictions of the most influential AI players, it is visible through already established AI initiatives that even though there are certain strong differences in prioritizing data protection and cybersecurity of big data, there is no direct mutual exclusion. The differences in priorities such as the EU wanting stronger regulation at the cost of innovation and the US wanting less regulation for innovation to flourish can be overcome with possible global solutions, i.e., further exploration of privacy-preserving solutions which could allow the advanced collection and safe usage of data for innovation while preserving the privacy of data subjects. Therefore, it seems that at least in the context of data protection and cybersecurity of big data, there could be an agreement among the EU, the US, and China, thus influencing the rest of the countries worldwide to law down the necessary framework for

[258] Men, 'Between Human Rights and Sovereignty: An Examination of EU–China Political Relations'.

ethical AI global governance with the help of other global AI initiatives with the focus on privacy and security.

This is important for establishing an urgently needed legally binding global framework to tackle global solutions with global joint efforts that is universal no matter the cultural differences, which could also serve as an important precedent for regulating other upcoming emerging technologies. Thus, no arms race should be more critical than human-centric innovation, sustainability, and peace. Therefore, global governance on AI should focus on similarities in the identified regulatory patterns, transcend cultural and national priority differences and aim for universal safeguarding of human rights in the age of AI, especially of the right to privacy, through solid data protection and cybersecurity of AI. This can be only possible with enormous efforts and open communication from all sides, especially from the Eu, the US, and China as three leading AI global trendsetters with international influence, and further research on the possibility of ethical global AI governance despite cultural differences in understanding human rights and for example, the right to privacy.

To conclude, this thesis research accomplished the aim of selecting and comparing the main legal instruments and policy plans of the EU, the US, and China relevant to data protection and cybersecurity in AI on which the ethical, global agenda or governance in the context of privacy be built and finding the similarities in the regulatory framework patterns on with the following conclusion:

(1) legal and policy regulatory frameworks have challenges to keep pace with AI innovation, including data protection and cybersecurity of the AI supply chain provisions relevant for AI governing both on the national and international level;

(2) despite different detected key prioritization (human rights/industry/national security) within jurisdictions, all currently developed national policies and plans on AI have a special section for achieving trustworthy AI related to preserving data privacy and security;

(3) selected jurisdictions rely on the private sector to led AI innovation development, which on the other hand seeks easing of the regulatory framework, especially when it comes to accessing data for the AI that feeds on big data;

(4) among others, AI innovation and development is the most important key driver for mutual collaboration between states, followed by interest to preserve human rights such as the right to privacy and data protection and challenges on how to achieve it without overregulating the private sector;

(5) currently, there is more focus set on developing national regulatory frameworks and plans than to participate in setting up the basis for ethical global governance or agenda on AI, which could result in a very much needed treaty relevant for data privacy and security;

(6) at the moment, examined jurisdictions prioritize the creation of national regulatory frameworks, agendas, and priorities with a rising trend to spread to international affairs as well as participating in the global initiatives and organizations when it comes to AI and AI challenges, including data privacy and security;

(7) shared tendency to become the most developed AI power globally (AI leadership), including the field of AI innovation and AI lawmaking and policymaking;

(8) while the scope and level of protection differs when it comes to data protection within selected jurisdictions, there is more or less a direct recognition of data protection either as a human right or a consumer right, thus impactful enough to further direct national plans and agenda on AI;

(9) the Brussels effect is present in the topic of data protection, as visible with the EU's GDPR example and its global influence, thus making way for further normative influence for the EU globally with the AI policy;

(10) existence of soft law versus hard law challenges either on the supranational level within differentiating opinion of members states on the 'law hardness' (the EU), lack of hard law on the federal level (the US), or lack of legally-binding legislation that appropriately safeguard the personal data (China).

This thesis research aimed to humbly contribute to the available research on global governance on AI that yet has to be more researched and developed in order to successfully plan, execute and monitor a human-centric approach to AI and the rest of disruptive and emerging technology that is yet to come, and that is urgently needed to be brought in order to safeguard human rights, especially the right to privacy as well as the security of the data.

BIBLIOGRAPHY

PWC. '2018 AI Predictions: Eight Insights to Shape Business Strategy'. Accessed 1 March 2021. https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions.html.

'Action Document for an International Alliance for a Human-Centric Approach to Artificial Intelligence (Annex 4)'. European Commission, 7 May 2019. https://ec.europa.eu/fpi/sites/default/files/annexe_4_human-centric_approach_to_artificial_intelligence_nlw_part1_v2.pdf.

Artificial Intelligence Security Standardization White Paper (2019 Edition) (2019). Unofficial English translation by Etcetera Language Group, Inc., < https://cset.georgetown.edu/wp-content/uploads/t0121_AI_security_standardization_white_paper_EN.pdf.

Bach, David, and Abraham Newman. 'The European Regulatory State and Global Public Policy'. *Journal of European Public Policy - J EUR PUBLIC POLICY* 14 (1 September 2001): 827–46. https://doi.org/10.1080/13501760701497659.

Bahar, Michael, Alexander Sand, and Mary Jane Wilson-Bilik. 'California's GDPR Has Become Law'. *JD Supra, LCC* (blog), 2 July 2018. https://www.jdsupra.com/legalnews/california-s-gdpr-has-become-law-94942/.

Banarjee, Krishendu. 'Can Global Alliance Stop China Becoming Artificial Intelligence Superpower?' International Business Times, 7 September 2020. https://www.ibtimes.sg/can-global-alliance-stop-china-becoming-artificial-intelligence-superpower-51268.

Bignami, Francesca. 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining'. *Boston College Law Review* 609, no. 48 (2007). https://lawdigitalcommons.bc.edu/bclr/vol48/iss3/3.

Bird, Richard. 'China "Standardises" AI Ethics'. Freshfields Bruckhaus Deringer, 26 January 2021. https://technologyquotient.freshfields.com/post/102gpfp/china-standardises-ai-ethics.

Bracy, Jedidah. 'Takeaways from New White House Annual Report on AI'. *International Association of Privacy Professionals* (blog), 27 February 2020. https://iapp.org/news/a/takeaways-from-new-white-house-annual-report-on-ai/.

Cadwalladr, Carole. '"I Made Steve Bannon's Psychological Warfare Tool": Meet the Data War Whistleblower'. *The Guardian*, 18 March 2018, sec. News. http://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

California Consumer Privacy Act, California Civil Code § (2018). https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf.

State of California, Department of Justice, Office of the Attorney General. 'California Consumer Privacy Act (CCPA)', 15 October 2018. https://oag.ca.gov/privacy/ccpa.

Cao, Deborah. *Chinese Law: A Language Perspective*. 2004.

Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Court of Justice of the European Union 16 July 2020).

Case C-498/16 Maximillian Schrems v Facebook Ireland Limited (Court of Justice of the European Union 16 July 2020).

Cavoukian, Anna, and Daniel Castro. 'Big Data Nad Innovation, Setting the Record Straight: Anonymization Does Work'. *Information and Privacy Commissioner Ontario Canada and Information Technology and Innovation Foundation*, 2014. https://www2.itif.org/2014-big-data-deidentification.pdf.

Charter of Fundamental Rights of the European Union (2007/C 303/01) (2007).

Chen, Albert Hung-yee. 'An Introduction to the Legal System of the People's Republic of China.' *LexisNexis*, 2011.

DataGuidance. 'China: TC260 Releases Cybersecurity Practice Guide on AI Ethical Security Risk Prevention', 12 January 2021. https://www.dataguidance.com/news/china-tc260-releases-cybersecurity-practice-guide-ai.

Chorzempa, Martin, Paul Triolo, and Sam Sacks. 'China's Social Credit System: A Mark of Progress or a Threat to Privacy?' *PIIE* (blog), 25 June 2018. https://www.piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy.

Chow, Vincent, and Barbara Li. 'Podcast #23: China's First Comprehensive Personal Data Law'. China Law and Practice, 13 November 2020. https://www.chinalawandpractice.com/2020/11/13/podcast-23-chinas-first-comprehensive-personal-data-law-barbara-li-rui-bai-law-firm/.

Cobb, Stephen. 'Data Privacy and Data Protection: US Law and Legislation'. *ESET White Paper CISSP*, 26 April 2016, 8.

Cohen, Neal. 'The Ethical Use of Personal Data to Build Artificial Intelligence Technologies: A Case Study on Remote Biometric Identity Verification'. *Carr Center Discussion Paper Series* 2020–004 (4 April 2020). https://carrcenter.hks.harvard.edu/files/cchr/files/200228_ccdp_neal_cohen.pdf.

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

Convention on Cybercrime, Pub. L. No. Treaty No.185 (2004). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Craig, Paul, and Gráinne de Búrca. *EU Law: Text, Cases, and Materials*. *EU Law*. 4th ed. Oxford University Press, 2007. https://www.oxfordlawtrove.com/view/10.1093/he/9780198714927.001.0001/he-9780198714927.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 'Defining Cybersecurity'. *Technology Innovation Management Review* 4 (30 October 2014): 13–21. https://doi.org/10.22215/timreview/835.

Creemers, Rogier, Paul Triolo, and Graham Webster. 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)'. DIGICHINA, 29 June 2018. http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

Crider, Cori. 'Mapping Regulatory Proposals for Artificial Intelligence in Europe'. AccessNow, 2018. https://www.accessnow.org/cms/assets/uploads/2018/11/mapping_regulatory_proposals_for_AI_in_EU.pdf.

Cybersecurity Standard Practice Guide: Guidelines for Artificial Intelligence Ethical Security Risk Prevention (2021). Unofficial English translation made available with Google Translate, https://www.tc260.org.cn/upload/2021-01-05/1609818449720076535.pdf.

Davenport, Thomas H., Jeanne Harris, and Jeremy Shapiro. 'Competing on Talent Analytics'. *Harvard Business Review*, 1 October 2010. https://hbr.org/2010/10/competing-on-talent-analytics.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (n.d.).

'DLA Piper: Data Protection Laws of the World'. Accessed 1 June 2021. https://www.dlapiperdataprotection.com/.

Electronic Communications Privacy Act, Pub.L. 99–508§ § (1986).

'Equality and Human Rights Commission: What Is the Charter of Fundamental Rights of the European Union?' Accessed 4 June 2021. https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union.

European Commission. 'Communication from the Commission to the European Parliament, the European Council, the Council the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe', 25 April 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN.

———. 'Communication from the European Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Coordinate Plan on Artificial Intelligence', 7 December 2018. file:///C:/Users/dalia/AppData/Local/Temp/com_2018_795_f1_communication_from_commission_to_inst_en_v6_p1_1003548_518E432D-A6F4-058B-35DBC88DF765593E_56018.pdf.

———. 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust', 19 February 2020. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Commission, Council of the European Union. Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 Final § (2021). https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

European Commission, High-Level Expert Group on AI. 'Ethics Guidelines for Trustworthy Artificial Intelligence', 8 April 2019. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

'European Data Protection Board: Who We Are'. Accessed 15 May 2021. https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en.

European Union. Treaty on the Functioning of the European Union, Pub. L. No. OJ L. 326/47-326/390; 26.10.2012 (2012). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

European Union Agency For Cybersecurity. 'AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence', 21 2020. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

European Union. 'European Union: Regulations, Directives and Other Acts'. Accessed 3 June 2021. https://europa.eu/european-union/law/legal-acts_en.

Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence (2019). https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.

Feinstein, Dianne. Cybersecurity Information Shaqring Act (2015).

Ferrándiz, Ester Mocholí, and Sara Degli-Esposti. 'After the GDPR: Cybersecurity Is the Elephant in the Artificial Intelligence Room'. *European Business Law Review* 32, no. 1 (1 February 2021). https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/32.1/EULR2021001.

'Final Report for the European Commission: Fundamental Rights Review of the EU Data Collection Instruments and Programmes'. Fondazione Giacomo Brodolini, 2018.

'Final Report: National Security Commission on Artificial Intelligence'. National Security Commission on Artificial Intelligence, 2021. https://www.nscai.gov/2021-final-report/.

Finley, Klint. 'Obama Wants the Government to Help Develop AI'. *Wired*, 10 February 2016. https://www.wired.com/2016/10/obama-envisions-ai-new-apollo-program.

'First Draft of the Recommendation on the Ethics of Artificial Intelligence'. UNESCO, 7 September 2020. https://unesdoc.unesco.org/ark:/48223/pf0000373434.

Fjeld, Jessica, Nele Achten, Hannah Hilligoss, Adam Nagy, and Madhulika Srikumar. 'Principled Artificial Intelligence: MappingConsensus in Ethical and Rights-Based Approaches to Principles for AI'. *Berjman Klein Center for Internet & Society*, 2020. https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=y.

Fung, Brian. 'The House Just Voted to Wipe Away the FCC's Landmark Internet Privacy Protections'. *Washington Post*, 29 March 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/.

Gal, Danit. 'China's Approach to AI Ethics'. Nesta Innovation Foundations, 18 May 2020. https://www.nesta.org.uk/report/chinas-approach-to-ai-ethics/.

Giardino, Elisa. 'The Mirage of a Global Framework for AI Governance'. *CARRE4* (blog), 7 November 2020. https://medium.com/carre4/the-mirage-of-a-global-framework-for-ai-governance-35b88a36615c.

'Global Artificial Intelligence Industry Whitepaper'. Deloitte, 2019. https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/global-ai-development-white-paper.html.

'Global Governance and Global Rules for Development in the Post-2015 Era'. United Nations, Economic & Social Affairs, 2014. https://www.un.org/en/development/desa/policy/cdp/cdp_publications/2014cdppolicynote.pdf.

González Fuster, Gloria, and Raphaël Gellert. 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right'. *International Review of Law, Computers & Technology* 26 (1 March 2012): 73–82. https://doi.org/10.1080/13600869.2012.646798.

Gordon, Lawrence A., and Martin P. Loeb. 'The Economics of Information Security Investment'. *ACM Trans. Inf. Syst. Secur.* 5, no. 4 (2002): 438–57.

'GPAI Frequently Asked Questions'. Accessed 10 June 2021. https://www.gpai.ai/about/.

Green, Bryan A. 'Lessons from the Montreal Protocol: Guidance for the Next International Climate Change Agreement'. *Environmental Law* 39, no. 1 (2009): 253–83.

Groussot, Xavier, Laurent Pech, and Gunnar Thor Petursson. 'The Scope of Application of Fundamental Rights on Member States' Action: In Search of Certainty in EU Adjudication', 1 July 2011. https://doi.org/10.2139/ssrn.1936473.

Grüll, Philipp. 'Germany Calls for Tightened AI Regulation at EU Level'. *EURACTIV* (blog), 30 June 2020. https://www.euractiv.com/section/digital/news/germany-calls-for-tightened-ai-regulation-at-eu-level/.

Gruschka, Nils, Vasileios Mavroeidis, Kamer Vishi, and Meiko Jensen. *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*, 2018. https://doi.org/10.1109/BigData.2018.8622621.

Hagendorff, Thilo. 'The Ethics of AI Ethics: An Evaluation of Guidelines'. *Minds and Machines* 30 (1 March 2020). https://doi.org/10.1007/s11023-020-09517-8.

Harari, Yuval Noah. 'Nationalism vs. Globalism: The New Political Divide'. World Bank Group. *Olc.Worldbank.Org* (blog), 2017. https://olc.worldbank.org/content/yuval-noah-harari-nationalism-vs-globalism-new-political-divide.

Harper, Jim. 'A Twenty-First Century Framework for Digital Privacy: Balancing Privacy and Security in the Digital Age'. *National Constitution Center* (blog). Accessed 20 March 2021. https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age.

Heikkila, Melissa. 'Europe Eyes Strict Rules for Artificial Intelligence'. *POLITICO*, 14 April 2021. https://www.politico.eu/article/europe-strict-rules-artificial-intelligence/.

US Legal Definitions. 'Invasion of Privacy Law and Legal Definition by USLegal, Inc.' Accessed 20 April 2021. https://definitions.uslegal.com/i/invasion-of-privacy/.

Jehl, Laura, and Alan Friel. 'CCPA and GDPR Comparison Chart | Practical Law'. Thomson Reuters Practical Law, 2018. https://content.next.westlaw.com/Document/If5ef6c05be5b11e8a5b3e3d9e23d7429/View/FullText.html?transitionType=Default&contextData=(sc.Default).

Jolly, Ieuan. 'Data Protection in the United States: Overview'. Thomson Reuters Practical Law, 2017. https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?transitionType=Default&contextData=(sc.Default).

Junru, Li. 'Understanding Human Rights: An Issue in EU-China Relations'. *EU-China Observer College of Europe*, no. 4 (2009). https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjgn7avx7_xAhUCgf0HHZbTBEsQFjAAegQIAxAD&url=https%3A%2F%2Fwww.coleurope.eu%2Fsystem%2Ffiles_force%2Fresearch-paper%2Feu_china_observer_4_2009.pdf%3Fdownload%3D1&usg=AOvVaw1gVe2DLuU3e2PZhTi7LCLx.

Kiljunen, Kimmo. *The European Constitution in the Making*, 2004. http://www.ceps.be/book/eu-constitution.

Kim, Graham Webster, Scarlet. 'The Data Arms Race Is No Excuse for Abandoning Privacy'. *Foreign Policy* (blog), 14 August 2018. https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/.

Klau, Daniel. 'Privacy, Security, and the Legacy of 9/11'. *UConn Today* (blog), 10 September 2015. https://today.uconn.edu/2015/09/privacy-security-and-the-legacy-of-911/.

Laskai, Samm Sacks, Lorand. 'China Is Having an Unexpected Privacy Awakening'. Slate Magazine, 7 February 2019. https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html.

Lawrence, Brenda L. Executive Order: Supporting the development of guidelines for ethical development of artificial intelligence. (2019). https://www.congress.gov/bill/116th-congress/house-resolution/153/text.

———. Supporting the Development of Guidelines for Ethical Development of Artificial Intelligence (2019). https://www.congress.gov/bill/116th-congress/house-resolution/153/text.

Li, Tiffany C., Jill Bronfman, and Zhou Zhou. 'Saving Face: Unfolding the Screen of Chinese Privacy Law'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 1 August 2017. https://papers.ssrn.com/abstract=2826087.

Loeb, Lawrence A. Gordon and Martin P. 'You May Be Fighting the Wrong Security Battles'. *Wall Street Journal*, 26 September 2011, sec. Tech. https://online.wsj.com/article/SB10001424053111904900904576554762089179984.html.

Lucas, Louise. 'China's Artificial Intelligence Ambitions Hit Hurdles'. *Financial Times*, 15 November 2018. https://www.ft.com/content/8620933a-e0c5-11e8-a6e5-792428919cee.

Lucero, Karman. 'Artificial Intelligence Regulation and China's Future'. *Columbia Journal of Asian Law* 33, no. 1 (31 December 2019): 94–171. https://doi.org/10.7916/cjal.v33i1.5454.

Ma, Ying, Yandong Zhao, and Miao Liao. 'The Values Demonstrated in the Constitution of the People's Republic of China'. In *Science and Technology Governance and Ethics: A Global Perspective from Europe, India and China*, edited by Miltos Ladikas, Sachin Chaturvedi, Yandong Zhao, and Dirk Stemerding, 73–81. Cham: Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-14693-5_6.

Manheim, Karl M., and Lyric Kaplan. 'Artificial Intelligence: Risks to Privacy and Democracy'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 25 October 2018. https://papers.ssrn.com/abstract=3273016.

Marr, Bernand. 'Why Only One of the 5 Vs of Big Data Really Matters'. *IBM BIG DATA & ANALYTICS HUB* (blog), 19 March 2015. http://www.ibmbigdatahub.com/blog/why-only-one-5-vs-big-data-really-matters.

McLuhan, Marshall, and Bruce Powers. *The Global Village: Transformations in World Life and Media in the 21st Century*. Oxford University Press, 1989.

Medhora, Rohinton. 'AI & Global Governance: Three Paths Towards a Global Governance of Artificial Intelligence - United Nations University Centre for Policy Research'. *United Nations University Centre for Policy Research* (blog). Accessed 7 June 2021. https://cpr.unu.edu/publications/articles/ai-global-governance-three-paths-towards-a-global-governance-of-artificial-intelligence.html.

Meehan, Mary. 'Data Privacy Will Be The Most Important Issue In The Next Decade'. *FORBES*, 26 November 2019. https://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-important-issue-in-the-next-decade/.

Mehmood, A., Iynkaran Natgunanathan, Yong Xiang, Guang Hua, and Song Guo. 'Protection of Big Data Privacy'. *IEEE Access*, 9 May 2016. https://doi.org/10.1109/ACCESS.2016.2558446.

Men, Jing. 'Between Human Rights and Sovereignty: An Examination of EU–China Political Relations'. *European Law Journal* 17, no. 4 (July 2011): 534–50.

Meredith, Sam. 'Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal'. CNBC, 10 April 2018. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

'Ministerial Statement on Trade and Digital Economy'. G20, 2019. https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf.

Moore, Gordon. 'Cramming More Components onto Integrated Circuits'. *Electronics Magazine* 38, no. 8 (19 April 1965). https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf.

Moschell, Ryan. 'And There Was One: The Outlook for A Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection'. *Texas Tech Law Review* 37, no. 2 (2004): 357–432.

New Generation Artificial Intelligence Development Plan (2017). English translation provided by NEW AMERICA and translators Rogier Creemers from Leiden Asia Centre, Graham Webster from Yale Law School, Paul Tsai from China Center, Paul Triolo from Eurasia Group and Elsa Kania. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017.

'OECD.AI Database of National AI Policies Powered by European Commission and OECD'. Accessed 24 June 2021. https://oecd.ai.

Pamphlet No. 14 of the United Nations Guide for Minorities: The European Union: Human Rights and the Fight Against Discrimination (2011). https://www.ohchr.org/en/issues/minorities/pages/minoritiesguide.aspx.

Parker, Lynne. 'The American AI Initiative: The U.S. Strategy for Leadership in Artificial Intelligence'. *OECD.AI Blog* (blog), 11 June 2021. https://oecd.ai/wonk/the-american-ai-initiative-the-u-s-strategy-for-leadership-in-rtificial-intelligence.

Periche, Jean Garcia. 'Artificial Intelligence and the Future of Global Governance'. *AI Policy Exchange* (blog), 7 August 2020. https://aipolicyexchange.org/2020/08/07/artificial-intelligence-and-the-future-of-global-governance/.

Pernot-Leplay, Emmanuel. 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?', 8 January 2020. https://www.researchgate.net/publication/337103856_China%27s_Approach_on_Data_Privacy_Law_A_Third_Way_Between_the_US_and_the_EU.

https://www.nortonrosefulbright.com/en/knowledge/publications/imported/2018/07/18/05. 'Personal Information Security Specification Commentary'. Norton Rose Fulbright. Accessed 3 March 2021. https://www.nortonrosefulbright.com/en/knowledge/publications/f959f04d/personal-information-security-specification.

Personal Information Security Specification (GB/T 35273-2017) (2020). Unofficial English translation available at www.ChineseStandard.net.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), Pub. L. No. COM/2020/767 final (2020).

Qi, George, Li Quianquian, Gretchen Ramos, and Darren Abernethy. 'China Releases Draft Personal Information Protection Law'. *The National Law Review* 11, no. 21 (21 January 2021). https://www.natlawreview.com/article/china-releases-draft-personal-information-protection-law.

'Recommendation of the Council on Artificial Intelligence OECD/LEGAL/0449'. OECD, 22 May 2019. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

'Report: Artificial Intelligence and Privacy'. Datatilsynet The Norwegian Data Protection Authority, 2018. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

'Report on Data Protection Law: An Overview R45631'. Congressional Research Service, 25 March 2019. https://fas.org/sgp/crs/misc/R45631.pdf.

Riazati, Saba. 'A Closer Look: Professor Seeks Stronger UN'. The Daily Bruin, 17 October 2006. https://dailybruin.com/2006/10/17/a-closer-look-professor-seeks.

Roberts, Huw, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi. 'The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 1 September 2019. https://doi.org/10.2139/ssrn.3469784.

Ros, Taylor. 'The Good, the Bad and the Ugly Arguments for Ditching the EU Charter of Fundamental Rights'. *LSE BREXIT* (blog), 1 February 2018. https://blogs.lse.ac.uk/brexit/2018/02/01/the-good-the-bad-and-the-ugly-arguments-for-ditching-the-eu-charter-of-fundamental-rights/.

Ruan, Lotus. *When the Winner Takes It All: Big Data in China and the Battle for Privacy*. Australian Strategic Policy Institute, International Cyber Policy Institute, 2018. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-06/Winner%20takes%20it%20all.pdf?_xjatw9CjqVHU018uCRZ6mOG4XAuYy8G=.

Russel, Stuart, and Peter Norvig. *Artificial Intelligence: A Modern Approach*. 3rd ed. Pretice Hall Press, 1995.

S. and Marper v. the United Kingdom (2008) ECHR (European Court of Human Rights (Grand Chamber) 4 December 2008).

Sacks, Sam. 'China's Emerging Data Privacy System and GDPR'. *Center for International and Strategic Studies* (blog), 8 March 2018. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

Saslow, Kate. 'Understanding US Federal AI Policy: Recommitting to a Transatlantic Coalition on AI'. Stiftung Neue Verantwortung, 23 November 2020. https://www.stiftung-nv.de/de/publikation/understanding-us-federal-ai-policy-recommitting-transatlantic-coalition-ai.

Schwartz, Ari, Deirdre Mulligan, and Indrani Mondal. 'Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues'. *A Journal of Law and Policy for the Information Society* 1 (2005).

Selby, John. 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?' *International Journal of Law and Information Technology* 25 (1 September 2017): 213–32. https://doi.org/10.1093/ijlit/eax010.

'Snapshot'. Accessed 30 June 2021. https://olc.worldbank.org/content/yuval-noah-harari-nationalism-vs-globalism-new-political-divide.

Steiner, Jo, Lorna Woods, and Christian Twigg-Flesner. *EU Law*. 9th ed. Oxford University Press, 2006. https://www.amazon.com/EU-Law-Jo-Steiner/dp/0199279594.

Stolton, Samuel. 'EU Nations Call for "Soft Law Solutions" in Future Artificial Intelligence Regulation'. *EURACTIV*, 8 October 2020. https://www.euractiv.com/section/digital/news/eu-nations-call-for-soft-law-solutions-in-future-artificial-intelligence-regulation/.

Stored Communications Act 18 U.S.C. Chapter 121 §§ 2701–2712 (n.d.).

Sullivan, Clare. 'EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era'. *Computer Law & Security Review* 35, no. 4 (1 August 2019): 380–97. https://doi.org/10.1016/j.clsr.2019.05.004.

Tedeneke, Alem. 'World Economic Forum Launches New Global Initiative to Advance the Promise of Responsible Artificial Intelligence'. *World Economic Forum* (blog), 28 January 2021. https://www.weforum.org/press/2021/01/world-economic-forum-launches-new-global-initiative-to-advance-the-promise-of-responsible-artificial-intelligence/.

Tene, Omer, and Jules Polonetsky. 'Big Data for All: Privacy and User Control in the Age of Analytics'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 20 September 2012. https://papers.ssrn.com/abstract=2149364.

'The History of the General Data Protection Regulation | European Data Protection Supervisor'. Accessed 1 May 2021. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update (2019). https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

'The U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools'. National Institute of Standards and Technology, the US Department of Commerce, 9 August 2019. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

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

Timmers, Paul. 'Ethics of AI and Cybersecurity When Sovereignty Is at Stake'. *Minds and Machines* 29, no. 4 (1 December 2019): 635–45. https://doi.org/10.1007/s11023-019-09508-4.

Translate, China Law. 'Outline for the Establishment of a Social Credit System'. *China Law Translate* (blog). China Law Translate, 27 April 2014. Unofficial English Translation available by China Law Translate,https://www.chinalawtranslate.com/socialcreditsystem/.

Tse, Siu Chung Dixon. 'Data Privacy Law: An International Perspective by Lee Andrew Bygrave'. *King's Law Journal* 25, no. 3 (31 December 2014): 497–99. https://doi.org/10.5235/09615768.25.3.497.

Turing, Alan. 'I.—COMPUTING MACHINERY AND INTELLIGENCE'. *Mind* LIX, no. 236 (1 October 1950): 433–60. https://doi.org/10.1093/mind/LIX.236.433.

'Unboxing AI: 10 Steps to Protect Human Rights'. Council of Europe, 2019. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.

United Nations Treaty Collection. Montreal Protocol on Substances that Deplete the Ozone Layer, § Chapter 27(2a) (1987). https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVII-2-a&chapter=27&clang=_en.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act), Pub. L. No. 107–56 (2001). https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf.

'US Criticised by UN for Human Rights Dailings on NSA, Guns and Drones'. *The Guardian*, 13 March 2014, sec. World news. http://www.theguardian.com/world/2014/mar/13/us-un-human-rights-abuses-nsa-drones.

Wagner. 'China's Cybersecurity Law: What You Need to Know', 12 December 2018. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

Wallace, Nick, and Daniel Castro. 'The Impact of the EU's New Data Protection Regulation on AI'. Center for Data Innovation, 27 March 2018. https://datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/.

Warren, Samuel D., and Louis D. Brandeis. 'The Right to Privacy'. *Harvard Law Review* 4, no. 5 (1890): 193–220. https://doi.org/10.2307/1321160.

Wassenhoven, Lidia. 'The Montreal Protocol on Substances That Deplete the Ozone Layer', 2 June 2006. https://theozonehole.com/montreal.htm.

European Commission. 'Why Do We Need the Charter?' Text. Accessed 30 April 2021. https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en.

Human Rights Watch. 'World Report 2020: Rights Trends in United States', 13 December 2020. https://www.hrw.org/world-report/2020/country-chapters/united-states.

Wright, Nicholas. 'How Artificial Intelligence Will Reshape the Global Order', 10 July 2018. https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

Zarsky, Tal. 'Incompatbile: The GDPR in the Age of Big Data'. *Seton Hall Law Review* 47, no. 4 (8 August 2017). https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.