Bachelor's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Humanities
Department of Historical and Classical Studies

Stephany Corlett Amdahl

# The European Union's GDPR and Data Protection Law in the U.S. and China

## A Multiple Case Study Analysis on the EU's Normative Influence.

Bachelor's thesis in European Studies with English
Supervisor: Carine Germond
May 2023

NTNU
Norwegian University of
Science and Technology

Stephany Corlett Amdahl

# The European Union's GDPR and Data Protection Law in the U.S. and China

## A Multiple Case Study Analysis on the EU's Normative Influence.

Bachelor's thesis in European Studies with English
Supervisor: Carine Germond
May 2023

Norwegian University of Science and Technology
Faculty of Humanities
Department of Historical and Classical Studies

NTNU
Norwegian University of
Science and Technology

# Abstract

Over the last decades, data privacy has become a major triggering issue globally. Therefore, in order to combat such a backdrop, the European Union (EU) adopted the General Data Protection Regulation (GDPR) in 2016. The regulation has as its main intent to safeguard the personal data of EU citizens via a complex and protective regulatory regime. However, the EU's GDPR has impacted not only its internal provisions, but it has also managed to normatively influence other data-privacy jurisdictions worldwide.

For that reason, this thesis provides a comparative analysis of the EU's normative influence on two data-privacy paradigms: the California Consumer Privacy Act (CCPA) and the Personal Information Protection Law (PIPL). By applying a Most Different Case Study Analysis, this paper qualitatively analyses 'how and to what extent' the EU's GDPR has normatively influenced the two legislations in question. The comparison is based on four dimensions: (1) territorial scope, (2) key terminology, (3) data subject rights, and lastly (4) enforcement and penalties. Conclusively, the thesis notes that the GDPR has served as a foundational blueprint for both the CCPA and PIPL, however, only to the extent it parallels with the American and Chinese internal and external interests.

# Sammendrag

I løpet av de siste tiårene har personvern blitt et betydelig problem på global skala. I 2016 vedtok EU en personvernslov kalt “General Data Protection Regulation” (GDPR) med formål å beskytte personopplysningene til europeere gjennom et komplekst og beskyttende reguleringsregime. Men, EUs GDPR har i tillegg påvirket interne bestemmelser, og jurisdiksjoner for personvern over hele verden.

På grunn av denne påvirkningen, inneholder denne fagteksten en sammenlignende analyse av EUs innflytelse på to personvernsparadigmer: “California Consumer Privacy Act” (CCPA) og “Personal Information Protection Law” (PIPL). Ved bruk av en saks studie analyse "Most different case study analysis", analyserer denne fagteksten hvordan og i hvilken grad EUs GDPR har normativt påvirket de to aktuelle lovgivningene. Sammenligningen er basert på fire punkter: (1) territorielt omfang, (2) viktige terminologier, (3) rettigheter for individer og (4) håndhevelse og straff. Avslutningsvis, legger fagteksten vekt på at EUs GDPR har fungert som en grunnleggende plan for CCPA og PIPL, men bare til den grad der interne interesser står parallelt med både de amerikanske og de kinesiske sine interesser.

# Table of Contents

# List of Tables



# List of Abbreviations

| | |
|---|---|
| EU | European Union |
| NPE | Normative Power Europe |
| GDPR | General Data Protection Regulation |
| CCPA | California Consumer Privacy Act |
| PIPL | Personal Information Protection Law |
| DPA | Data Protection Act |
| EC | European Community |
| DPD | Data Protection Directive |
| DPAs | Data Protection Authorities |
| CAC | Cyberspace Administration of China |

# 1 Introduction

One of the modern theories designed to characterize the nature of the European Union (EU) as an actor in international politics is the idea of *Normative Power Europe* (NPE) (Savaroskaya, 2015, p. 66). The concept revolves around the EU's ability to shape the international environment by producing changes in its standards, norms and procedures echoed in the EU's very own standards, values and procedures (Skolimowska, 2015, p. 112). Similarly, in light of the NPE, a recently developed concept - known as the *Brussels Effect* - further emphasizes the EU's role in the international setting. According to Bradford (2020), the concept characterizes the EU as an influential superpower that has a unilateral ability to modulate markets in the global business framework. Consequently, the EU promulgates "regulations that influence which products are built and how business is conducted, not just in Europe but everywhere in the world" (p. 14).

However, according to Diez & Manners (2007), this widely held belief that the EU is a "novel kind of power not only in its own institutional set-up but also in its external relations" does not go without contestation - hence, provoking debates and raising a number of questions. Although the European Union constitute a new kind of power in international politics, these authors argue, there are those who contest the EU's ability to influence the standards of other parts of the world, and therefore, the extent to which it can be called a "normative power" (p. 173). This interpretation and criticism come primarily from scholars of opposite or alternative theoretical paradigms, such as neo-realism (Skolimowska, 2015, p. 112). Nevertheless, according to Sjursen (2006), there might be some validity to such conceptualization of the European Union as a "normative power", and rather than being rejected, it should be closely analysed (p. 235). For that reason, this thesis attempts to further analyse and - to a certain extent - test such conceptualization in the face of the EU's ability to influence global markets in the area of digital economy - in particular, through the *General Data Protection Regulation* (*GDPR*).

Historically, there have been few regulations that have had a greater influence on global digital companies or their users than the European Union's GDPR (Bradford, 2020, p. 131). The regulation focuses essentially on a range of "individual rights designed to protect consumers whose personal information is collected, processed and stored by corporations and other entities" (Victor, 2013, p. 513). Throughout the previous several years, citizens' data privacy has become a worldwide triggering issue (Calzada, 2022, p. 1130). Although data security and privacy are argued to be a longstanding problem, the globalized expansion of digitalized economic means has gradually intensified the transborder information flow, where personal data came to be a critical corporate asset (Todt, 2019, p. 39). Under the circumstances of a hyperconnected data economy, personal data is constantly collected, compiled and eventually sold to other corporations by Big Tech companies (Victor, 2013, p. 517). As a result, consumers/citizens face the simultaneous need to protect their privacy and provide personal information in order to obtain a variety of services (Calzada, 2022, p. 1130).

Yet, according to Calzada (2022), alongside the GDPR, there are two other worldwide data privacy paradigms that currently exist against this backdrop in data privacy: the

*California Consumer Privacy Act* (CCPA), and the *Personal Information Protection Law* (PIPL) (p. 1129). In the wake of the EU's GDPR, in 2018, a staggering amount of privacy-related legislations have been adopted throughout the world (Gorostiza & McMillan, 2022, p. 2). Accordingly, both the CCPA and PIPL are instances of legislation pertaining to privacy that have been adopted subsequently to the EU's GDPR. In recognizing data as property, the state of California adopted the CCPA - a regional data protection legislation - in the United States in 2018; and China adopted the PIPL - a national data protection law - in 2021 (Calzada, 2022, p. 1130). Although implemented differently (as shown in section 4), the CCPA and PIPL present a great degree of resemblance to the GDPR, and therefore, are argued to be clearly derived from it (Reid, 2022). For that reason, in the context of the EU's normative power, it is believed that current legislations and events in privacy should be considered in a "post-GDPR" lens (Gorostiza & McMillan, 2022, p. 2).

In general, this thesis aims to identify characteristic features of the EU's GDPR in the American *CCPA* and the Chinese *PIPL* through a comparative analysis that goes over the content of the three jurisdictions, that is, through a multiple case study analysis. In analysing how and the extent to which the European Union has influenced both data-protection legislations through the GDPR, it is possible to closely examine the role of the European Union as a normative power in the international environment, particularly, in the area of digital economy. Correspondingly, the thesis is structured as followed. The first section reviews the literature review and methodology. The second section further conceptualizes the concepts of *Normative Power Europe* and *Brussels Effect*. The third section sets the tone for the GDPR's normative influence and briefly analysis the CCPA and PIPL's alignment factors. The fourth section compares the implementation of the three jurisdictions from the stance of four dimensions: (1) territorial scope, (2) key terminology, (3) data subject rights and (4) enforcement and penalties. The fifth and last section concludes with the main findings and limitations of this thesis.

## 1.1 Literature Review

In conditioning an analysis of the EU's normative influence in setting globally high standards and norms through the GDPR, it is important to provide a literature review that aims to produce an overview of the key theoretical and empirical contributions. Therefore, this literature review will be concerned with literature that focuses on the main conceptual frameworks explored in this thesis: *Normative Power Europe* and *Brussels Effect*. Alongside that, it will also briefly provide literature that opposes such frameworks; and finally, literature that provides, in its own parameters, analytical evidence of the GDPR's regulatory influence on the CCPA and PIPL.

To begin with, as a response to the significant growth of the European Union as a global actor, the concepts of *Normative Power Europe* and *Brussels Effect* have gained meaningful attention in the academic world. In understanding the NPE concept, one of the earliest and most influential works was written by Ian Manners (2002), who played a key role in popularising the subject matter (Noureddine, 2016). In his article, Manners (2002) provides a theoretical approach that entrenches the EU's identity with its role in international politics. Thereby, the author claims that the norms and values that constitute the EU's identity have a normative impact on the global environment (Manners, 2002, p. 252). Most recently, Bradford (2020) further developed the EU's

normative role in the international setting through the concept of *Brussels Effect* (first introduced by her in 2012). In her book, the author provides both theoretical and empirical approaches to the EU's regulatory power in the global arena. Overall, Bradford (2020) focuses on the EU's ability to promulgate its rules through its legal institutions and standards (p. 14).

As such, up to the present moment, the idea of the EU as a normative power has received not only praise but also a considerable amount of criticism in academia (Skolimowska, 2015, pp. 120-121). For instance, Lucarelli & Menotti (2006) emphasizes the lack of consistency between "the normative rhetoric and the *de facto* actions of the European Union in its international relations" (Skolimowska, 2015, p. 121). Whereas, Sjursen (2006) points out that the normative theory statements are rather vague and lack criteria and assessment standards that would help to qualify or reject the EU as a normative power. In addition to that, the author also draws attention to the fact that such a normative conception corresponds to a self-idealization and identification of the European Union rather than an actual fact (Skolimowska, 2015, p. 122). Yet, as mentioned in the introduction, Sjursen (2006) does not discard the EU's normativity but rather asks for a deeper and more specific analysis of such conceptualisation (p. 235).

Therefore, as this thesis attempts to further specify such a conception in light of the EU's digital normativity, literature that provides empirical evidence of the GDPR's influence on different privacy-related legislation around the world, particularly the CCPA and PIPL, is necessary. For example, Calzada (2022) compares through a "state-of-art" review the three main data privacy paradigms that currently exist: GDPR, CCPA and PIPL. By focusing on PIPL as the primary unit of analysis, the author states that the CCPA and, notably, the PIPL emulate the goals of the GDPR; and comes to the conclusion that the three data-privacy legislations are currently "influencing digital policies and practices worldwide", although PIPL's greater influence is yet to be seen (Calzada, 2022, p. 1145). Furthermore, Gorostiza & McMillan (2022) analyze the varying levels of success by "various governing bodies from around the world" on the imposition of different "regulatory efforts on the usage of internet by its citizens" (p. 1). Through a comprehensive analysis report, the authors examine not only the GDPR, CCPA and PIPL but also Zimbabwe's *Data Protection Act* (DPA). Conclusively, the authors assert that the GDPR constituted the prototype of every regulation effort displayed by them in the article; and that the GDPR as well as the PIPL are successful in impacting providers outside their own jurisdiction, whereas the CCPA and DPA have "little political power on the world stage" (Gorostiza & McMillan, 2022, p. 6).

All in all, this thesis sympathizes to a great extent with the *conceptual-framework* statements made by Manners (2002) and Bradford (2020), and it takes into consideration some of the arguments made by Sjursen (2006). Alongside that, it also draws on the analysis and conclusions made by Calzada (2022) and Gorostiza & McMillan (2022). Altogether, although several scholars and articles explore similar topics and research questions to this thesis, there is little to no literature that explicitly links the EU's normative power to the modern context of digital economy, particularly, in light of the GDPR's regulatory influence on the CCPA and PIPL. Alongside that, the little literature that simultaneously compares the content of the three legislations is somewhat superficial. Such literature limitation can be attributed to the considerably recent adoption of both the CCPA and PIPL. Therefore, this thesis contributes to the existing literature by filling this gap.

## 1.2 Methodology

This thesis will be primarily conducted as a *Multiple Case Study Analysis* with an emphasis on document/legislation review in order to perform its empirical evidence. For that matter, the main unit of analysis is the EU's normative influence through the GDPR which is examined based on two case studies: the CCPA and PIPL. Yet, according to Yin (2017), a multiple-case design is chosen so that "individual case studies either (a) predict similar results (a literal replication) or (b) predict contrasting results but for anticipatable reasons (a theoretical replication)" (p. 55).

In the case of the analysis carried out in this thesis, the intent is that the individual case studies selected predict, to a certain degree, similar results. Therefore, the accurate method which will be applied is known as the *Most Different Case Study Analysis* - that is, a comparative analysis that aims to "maximize the number of variables in which the system differs in order to investigate the phenomenon" (Enli, 2010, p. 13). For that reason, the intent is to not only qualitatively analyze but also to compare the American and Chinese data protection laws (CCPA & PIPL, respectively) in the light of the GDPR's normative power. Although the main focus is on the qualitative analyses, the independent variable (Y) in the comparison will be the countries' political/cultural differences; whereas, the dependent variable (X) will be the adoption of a similar privacy and data protection law based on their willingness to comply with EU legislation, that is, in the format of the GDPR. The connection between the dependent and independent variables is mainly attributed to the countries' market-driven economies and their respective national interests.

Consequently, the use of qualitative data will be turned into examining the extent to which both data-protection legislations were influenced by the GDPR. Thus, throughout the analysis, the use of primary and secondary sources is appropriate. The primary sources will mainly and firstly come from the three official legislations themselves: *General Data Protection Regulation* (GDPR), *California Consumer Privacy Act* (CCPA), and lastly, *Personal Information Protection Law* (PIPL) (PIPL's translated version by Creemers & Webster (2021)). Those will be used to provide empirical evidence where there will be a slight focus on comparative *document analysis* between the three legislations. Whereas, the secondary sources will come from journals, books, and others that will support the analysis, such as the ones in the *Literature Review*. Together, those sources will provide both with empirical and theoretical data that will help to answer the research question of this thesis.

# 2 EU's Normative Influence: *Normative Power Europe* (NPE) & The *Brussels Effect*

Normative Power Europe (NPE) and the Brussels Effect are two conceptual frameworks that seek to explain the EU's influence beyond its own borders. Yet, the two concepts reflect slightly different dimensions of the EU's global normativity. On the one hand, NPE highlights a mechanism that sees the EU's normative influence externalising its values and norms (Savorskaya, 2015, p. 66). Whereas, the Brussels Effect highlights a mechanism that sees the EU's normative influence externalising its legal and institutional standards (Bendiek & Stuerzer, 2023, p. 3). Nevertheless, according to Skoliwowska (2015), these two concepts do not automatically constitute divergent ideas but rather a conceptual evolution of the "normative power" notion:

> Since its formulation the concept of "a normative power" has evolved within the field of European Studies, and has been used to account for the transformation of institutional and legal circumstances and the conditions in which the European Union conducts its activity. (p. 128)

Therefore, the *Brussels Effect* concept would rather embody, to a certain extent, an evolution or even a variation of the *NPE* concept. Even though the NPE focuses on the normative influence of the EU's norms and values, while the Brussels Effect focuses on the normative influence of EU rules - such as the GDPR (Manners, 2002; Bradford, 2020); both concepts emphasize the EU's ability to: shape global governance and promote its values and standards. Together, the two concepts help to explain the multifaceted nature of the EU's global influence and, thereby, are the appropriate theoretical basis for this thesis.

## 2.1 Europe as an International Normative Power

Until the 1990s, the role of the previous European Community (EC) has been defined based on the categories of both "military power" and/or "civilian power" (Skolimowska, 2015, p. 115). In that respect, *military power* yielded the Community's ability to use military instruments and *civilian power* yielded its ability to use economic or civilian instruments of power (Forsberg, 2011, p. 1185). Yet, in 1992, due to the supranational development of European Integration through the Maastricht Treaty, the political landscape of international relations was enhanced with the advent of the European Union (Skolimowska, 2015, p. 115). Consequently, this qualitative change in "the nature of European Integration by bringing the European Union into existence and by changing the framework within which its political external relations were established" gave rise to a transformation of the theoretical approach as well (Skolimowska, 2015, p. 116). Therefore, in order to overcome the outdated debate concerning the EU's role in the global setting, the idea that the EU should rather be illustrated as a "normative power" was presented by Ian Manners (Savorskaya, 2015, p. 68).

### 2.1.1 Manner's *Normative Power Europe* (NPE)

In 2002, Manners, a Danish political scientist, wrote a seminal article where he introduced the notion of the EU as an "ideological power", a "power over opinion" and even a "power of example" (Forsberg, 2011, p. 1185), better known as *Normative Power Europe* (NPE). Essentially, Manners (2002) argues that it "is possible to think of the ideational impact of the EU's international identity/role as representing normative power" (p. 238).

Correspondingly, Manners (2002) continues his argument by claiming that the European Union's normativity results from its "historical evolution, its hybrid polity, and its constitutional configuration", and for that reason, it experiences a "normatively different basis for its relations with the world" (p. 252). Thereupon, by providing a theoretical approach, Manners divides his argument into two aspects: the EU's identity and its influence on world politics (Noureddine, 2016). In the first aspect, the author asserts that the Union's international identity constitutes a "new and different" normative political entity due to its elite-driven, treaty-based and legal order composition (Manners, 2002, p. 241). Respectively, its principles - such as respect for democracy, the rule of law and human rights (TEU, Article 21.1) - are emphasized in its identity. In the second aspect, Manners (2002) claims that the EU's normative identity "predisposes it to act normatively in world politics (p. 252). For this reason, it influences the international environment through its core identity principles where the most important factor in shaping its role as a global actor is not "what it does or what it says, but what it is" (Manners, 2002, p. 252).

## 2.2 Europe as an International Regulatory Power

Alongside that, since the early 1990s, the European Union has also been working towards "an ambitious project to build a European regulatory state" (Bradford, 2020. p. 7). In adopting uniform standards to safeguard the consumer's health and safety via harmonization regulations (TFEU, Article 169), the EU's common market has been integrated. Consequently, this internal intention of seeking market integration through regulation has had an "unintended" and increasing impact externally which led the EU to become a dominant force in international regulation (Bradford, 2020. p. 7). In that respect, according to Hadjiyianni (2021), Anu Bradford's *Brussels Effect* significantly advances our understating of "power" in modern societies, extending it beyond the idea of the EU as a mere "normative power" to a power also defined by "regulatory capacity and market forces" (p. 243).

### 2.2.1 Bradford's *Brussels Effect*

In 2012, Bradford, a Finnish-American author, introduced her view on the EU's normative role in the international setting through the concept of the *Brussels Effect*. According to this concept, the EU constitutes a unilateral regulatory power through its legal institutions and standards (Bradford, 2012, p. 3). Although deeply underestimated, the author argues, the Union successfully exports its regulatory influence to the rest of the world without the need to rely on international institutions or other nations' cooperation (Bradford, 2012, p. 1). Consequently, the EU has "a strong and growing ability to promulgate regulations that become entrenched in the legal frameworks of developed

and developing markets alike, leading to a notable "Europeanization" of many important aspects of global commerce" (Bradford, 2012, p. 1).

In 2020, Bradford wrote a book where she further examines the concept. In her book, the author analyzes the key factors and conditions whereby this externalization of the EU's standards takes place: (1) the EU's large consumer market - underpinned by its strong regulatory structures - requires foreign companies and businesses to comply with such standards "or else forgo the EU market entirely"; (2) the EU's inelastic regulatory consumer market does not allow companies to circumvent "EU rules by moving regulatory targets to another jurisdiction"; and lastly (3), the preference by multinational companies to standardize and adhere a single rule "as opposed to customizing their production to each individual market" facilitates the EU's regulatory predominance (Bradford, 2020, pp. 14-15). In total, those factors and conditions summarize the Brussels Effect's five cumulative elements: market size, regulatory capacity, stringent regulations, inelastic targets and non-divisibility (Bradford, 2020, pp. 25-65).

Additionally, Bradford also terms the voluntary (or semi-voluntary) adherence to EU standards by foreign corporations as a "de facto Brussels Effect"; whereas, the adherence to EU-style regulations by foreign governments - as a result of pressure from domestic corporations or not - is termed as a "de jure Brussels Effect" (Bygrave, 2021, p. 5). Respectively, the author provides in her book empirical evidence of the "de facto" and the "de jure" Brussels Effect through several areas of regulatory policy where the EU set standards, such as market competition, consumer health and safety, the environment, and most importantly to this thesis, digital economy (Bradford, 2020).

Overall, both the NPE and the Brussels Effect bring about important aspects of the EU's normativity today. In this thesis, Manner's NPE will be implicitly presented through the founding principles and values of the European project brought about through the GDPR. Whereas, as complementary to the NPE, Bradford's Brussels Effect presents itself as a rather "diffusional mechanism" where norms and values of the EU are spread through the GDPR's regulatory standards and legal dimensions that ultimately influence other jurisdictions (de jure) around the world.

# 3 EU's Digital Normativity: The *General Data Protection Regulation* (GDPR)

Over the last two decades, a rapidly-expanding phenomenon has been transforming our societies: *digitalization*. This phenomenon presents the digitalization of economic practices and activities, which occurs through the incorporation of data and online platforms, as a key feature of contemporary times (IMF, 2018, p. 6). Nevertheless, such digital innovations bring both opportunities and challenges that, according to Amuso et.al (2019), require a "multilevel intervention that starts locally and becomes progressively global" (p. 125). In regard to new challenges surrounding data protection, the European Union has been gradually influencing global digital companies (de facto) and economies (de jure) through the *General Data Protection Regulation* (GDPR) (Bradford, 2020, p. 131).

In 2016, the EU adopted the GDPR - a "data governance framework" which encourages companies to "think carefully" about the data of individuals (Hoofnagle et.al, 2019, p. 67). Although only enforceable since 2018, the GDPR has had the purpose of protecting European citizens against the wrongful collection, operation and storage of personally identifiable information by corporations and any other entities that conduct business in EU territory (Victor, 2013, p. 513). In fact, much of the GDPR's pronounced features were mirrored in previous legislation - the Data Protection Directive (DPD), also known as the EU Directive 95/46 (EDPS, n.d). Yet, the *Directive* had poor enforcement and a relatively weak compliance and penalty mechanism (Hoofnagle et.al, 2019, p. 66). As a result, in an effort to tackle these and other flaws, the GDPR's updated "enforcement mechanisms, penalty determination, expanded security incident notification, and procedural requirements" - with the effect of identifying legal transgressions - rather discourage executives from viewing privacy breaches as mere "parking tickets" (Hoofnagle et.al, 2019, pp. 68, 71).

Indeed, the GDPR takes data privacy so seriously that it constitutes one of the "strictest and most detailed data protection regulations" in the world (Bendiek & Stuerzer, 2023, p. 14). Such a protective regulatory system can be attributed to the EU's recognition of personal data protection as a fundamental right (Gur, 2020, p. 314). According to Article 8 of the EU Charter of Fundamental Rights ("the Charter"), everyone has "the right to the protection of personal data concerning him or her" where "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned" (FRA, 2007). This legally binding fundamental right enforces the founding principles of the European project - such as dignity, respect, equality and fairness - that set the functional standards of the EU today (FRA, n.d). Hence, the founding norms and values, that the inalienable right to data protection embodies, can be claimed to be perpetuated in the legal standards of the GDPR (Custers & Malgieri, 2022, p. 9). Under those conditions, the EU sets "the tone globally for privacy and data protection regulation" (Bradford, 2020, p. 132).

As stated above, the EU's large consumer market places the Union in an influential position in the global economy (Bradford, 2020, p. 14). Consequently, its trading power strengthens the EU's "extraterritorial requests" and encourages states seeking to develop

cooperative agreements to implement standards and/or legislations similar to the EU (Gur, 2020, p. 315). In that matter, the EU makes use of a variety of measures in its relations with third countries to establish its influence in the field of data protection, such as adequacy and conditionality assessments (Gur, 2020, p. 315). According to the GDPR's Article 45(2), when granting an "adequacy decision" in the safe transfer of personal data to third countries, the EU checks the following criteria: (1) the respect for the rule of law, human rights and fundamental rights in the domestic legal system; (2) the existence of an effective supervisory authority; and (3) existent international commitments. Therefore, in order to have access to the EU's profitable consumer market, the "prospect of obtaining an adequacy decision by the EU" leads to the proliferation of GDPR-like jurisdictions, as well as the expansion of the EU's role as a fundamental rights actor and norm-setter in the global regulatory environment (Gur, 2020, p. 326).

To date, the European Union recognizes a few third countries as providing an adequate degree of data protection: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom, and Uruguay (European Commission, n.d.-a). Nevertheless, although the list continues to expand, there are a number of non-EU countries with jurisdictions that do not meet the EU "gold standard" of adequacy, but that was to a certain extent influenced to "align their laws with the GDPR" (Bradford, 2020, pp. 150-151), such as the United States and China.

## 3.1 GDPR's Normativity: The *California Consumer Privacy Act* (CCPA) & The *Personal Information Protection Law* (PIPL)

Both the U.S. and China have a long history of competing ideological, political, cultural and geographic differences that perpetuates to the present day (Allison, 2017, p. 81). However, the two countries have a "shared interest in promoting a strong and open global economy" in a way to further the interest of their people (The White House, 2015). Therefore, given the fact that the EU, the U.S. and China constitute the largest trading economies in the world, (digital) services and the respective transborder data flow between those economic blocs constitute an important aspect of their economic practices (European Commission, n.d.-b). At the same time, due to their dominant political and economic power, such cooperative trading parallels with competing data-related jurisdictions that seek "to extend their own normative influence" (Gur, 2020, p. 315). Nevertheless, the EU's GDPR has had a large impact on the formation of data protection legislation around the world and, according to Gorostiza & McMillan (2022), it has rather constituted a prototype for the American and Chinese regulatory efforts on data protection - particularly, the *California Consumer Privacy Act* (CCPA) and the *Personal Information Protection Law* (PIPL) (p. 3).

### 3.1.1 California's *CCPA*

On June 28, 2018, the State of California adopted the CCPA, and on January 1, 2020, the regulation became effective. The CCPA represents one of the first comprehensive data privacy legislations in the United States (Gunst, 2021, p. 8). As opposed to the EU, the United States does not acquire a single nation-wide data protection law; instead, it implements a series of state-wide legislation "to address specific issues and concerns related to data privacy" (Moreira, 2023, p. 11). In regards to the CCPA's implementation,

the legislation has as its main point the safeguarding of California residents' rights over their personal information handled by businesses - that is, like the GDPR, a rights-based approach (Moreira, 2023, p. 12). According to Moreira (2023), the legislation is a response to not only technological advancements but also to a "growing social movement against corporatism and the abuse of personal data by large companies" (p. 13).

With respect to the CCPA's alignment with the GDPR, the extent of EU-US data flow has led many American companies that already complied with the GDPR to support such coordination (Bradford, 2020, p. 151). The State of California is home to some of the biggest data-driven companies in the world, such as Facebook, Google and Apple (Gunst, 2021, p. 59). Therefore, in the absence of a federal law and the potential emergence of conflicting state privacy jurisdictions, those companies believe that a GDPR-equivalent legislation would rather ease their compliance efforts (Bradford, 2020, p. 149). For instance, Facebook's CEO Mark Zuckerberg has supported such alignment by stating that: "New privacy regulation in the United States and around the world should build on the protections GDPR provides" (Zuckerberg, 2019).

### 3.1.2 China's *PIPL*

On August 20, 2021, China adopted the PIPL, and on November 1, of the same year, the regulation became effective. Like the CCPA in the U.S., the PIPL also constitutes the first comprehensive legislation on data protection and data privacy in China (Luo & Wang, 2022). Yet, unlike the CCPA, the PIPL has its main focus on the protection of "the personal information of Chinese citizens from foreign companies and countries" rather than a focus on individual rights (Moreira, 2023, p. 1).

According to Daniel (2022), in aligning its national data protection law with the GDPR, the Chinese government rather enhances its control and monitoring over its citizens and its digital economic sector (p. 27). In contrast to the U.S.'s private-optimized system, the government in China plays a central role in guiding not only the economic but also the social spheres of the country - that is, a public-optimized system (Moreira, 2023, p. 15). Therefore, the fact that the GDPR provides a very strict legislation with a high level of governmental control makes it a suitable fit with the Chinese system (Bradford, 2020, p. 153). Alongside that, over recent years, there has been a series of high-profile data breaches where the personal information of millions of individuals has been lost. As a result, the concern about the ability of Chinese companies to protect the data of Chinese citizens against foreign "threats" has encouraged the Chinese government to implement a GDPR-like law (the PIPL) (Moreira, 2023, p. 16).

# 4 A Comparative Analysis of Global Data Privacy Regulations: GDPR, CCPA & PIPL

As stated above, the CCPA and PIPL do not acquire the GDPR's "gold standard" of adequacy. Yet, although the three legislations in question are not completely similar and to a certain extent would even constitute competing jurisdictions, this thesis draws upon the idea that the GDPR accounts for the CCPA and PIPL's archetype. Therefore, this essay develops a comparative analysis that aims to emphasize both the similarities and differences by referring back to the content of these three privacy regulations. The comparison has its base on the GDPR and, thereby, makes a simultaneous analysis between the GDPR, CCPA and PIPL. As shown in Table 1.1, the comparative analysis takes from the standpoint of four dimensions: (1) territorial scope, (2) key terminology relating to personal data and processing, (3) data subject rights and (4) enforcement and penalties.

**Table 1.1: Four-dimensional comparison of three data regulations.**

| **Dimension** | **GDPR** | **CCPA** | **PIPL** |
|---|---|---|---|
| **Territorial Scope** | All entities that process data of EU residents internally or externally. | All entities that process data of Californian residents internally or externally (it does not apply to companies that do not "do business" in California). | All entities that process data of Chinese residents internally or externally. |
| **Key Terminology: Personal Data & Processing** | ***Personal Data*** is "any information related to an identified or identifiable natural person ('data subject')". ***Processing*** is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, use, disclosure by | Both terms are similar to the GDPR (although the CCPA's definition of *personal data* adds Household data and its definition of *processing* lacks the categories displayed under the GDPR). | Both terms are similar to the GDPR's (although the PIPL's definition of *personal data* emphasizes anonymized information as not being personal data and its definition of *processing* is narrower than the GDPR's). |

| | | | |
|---|---|---|---|
| | transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction. (GDPR, Article 4) | | |
| **Data Subject Rights** | Right to access data, rectify data, erase data, data portability, objection, restrict processing and resist profiling. | All the rights mentioned in the GDPR, plus the right to opt-out the selling of personal data. | All the rights mentioned in the GDPR (although it lacks "GDPR language" and a clear 'exceptions' section). |
| **Enforcement & Penalties** | Data Protection Authorities (DPAs) as the supervisory authority + 10 to 20 million or 2% to 4% (annual turnover) fines depending on the severity of the violation. | The California Attorney General's Office as the supervisory authority + 2,500 USD and 7,500 USD fines for unintentional and intentional violations, respectively. | Multiple governmental departments (mentioned below) as the supervisory authority + 100,000 to 1 million Yuan fines for less severe breaches and up to 50 million Yuan or 5% (annual revenue) fines for more serious breaches. |

(Source: Calzada, 2022, p. 1139; Molnár, 2021, pp. 7-9.)

## 4.1 Dimension 1: Territorial Scope

To start with, *territorial scope* constitutes a critical dimension by which it is possible to measure the extent of the GDPR's normative influence on both the CCPA and PIPL. For instance, as with the GDPR, the territorial scope of both the CCPA and PIPL extends beyond the physical borders of their respective jurisdictions. Under the GDPR, corporations or any other entities based in EU territory are subject to the regulation for data processing activities (Article 3.1). Yet, the jurisdiction also stipulates that regardless of the company's location if it offers goods and services or it monitors the behaviour of individuals within the EU, those will also be subject to the GDPR for the processing of data of EU citizens (GDPR, Article 3.2).

Similarly, under the CCPA, entities that "do business in the State of California" are subject to the legislation, regardless of their location, when processing the data of California's residents (Cal. Civ. Code, §1798.140 (c)(1)). This requirement would correspond to the GDPR's: "activities of an establishment…in the Union" (GDPR, Article 3.1). Nevertheless, the CCPA does not apply to entities that do not "do business" in California, even though residents are being monitored, as long as such monitoring is not regarded as "doing business in California" (de la Torre, 2018).

Furthermore, under the PIPL, the law is applicable to activities related to data handling of "natural persons within the borders of the People's Republic of China" (Article 3). However, in case of data handling activities are to happen outside of Chinese borders, the law extends its territorial scope when the purpose is to: (1) provide products and services to natural persons inside China, (2) analyze or asses activities of natural persons inside China, or (3) other purposes specified by laws or regulations (PIPL, Article 3).

In general, even though the CCPA's applicable range appears to be relatively narrower when compared to the GDPR and PIPL, the three legislations present overall similar conduct in terms of (internal and external) territoriality (Calzada, 2022, p. 1140).

## 4.2 Dimension 2: Key Terminology (Personal Data and Processing)

As for the key terms, both *personal data* and the activities deemed as information *processing* are "two threshold definitions" (Hoofnagle et.al, 2019, p. 72). Therefore, it helps us to understand not only the basis for the GDPR but also the textual and conceptual influence it has had on both the CCPA and PIPL.

To begin with, according to the GDPR, the term *personal data* is defined as "any information related to an identified or identifiable natural person ('data subject')" (Article 4.1). While, the term *processing* is defined as being:

> Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction. (GDPR, Article 4.2)

Comparably, under the CCPA, *personal data* is termed as "personal information" and defined as "information that identifies, relates, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" (Cal. Civ. Code §1798.140 (o)(1)). Although comparatively similar, the GDPR and CCPA's definition of *personal data/information* mainly differs in that the CCPA's definition, unlike the GDPR's, includes extra-personal data - that is, not only data specific to individuals but also to households (Jehl & Friel, 2018, p. 2). Meanwhile, identically to the GDPR, the CCPA defines *processing* as "any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means" (Cal. Civ. Code §1798.140 (o)(2)). Yet, it lacks the categories, mentioned under the GDPR, exemplifying such an action.

Furthermore, under the PIPL, *personal data* is also termed as "personal information" and is ultimately defined as "all kinds of information recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling" (PIPL, Article 4). Despite its overall similarity, unlike the GDPR, the PIPL rather emphasizes that it does not deem anonymized data as being personal data (Ke et.al, 2021). In addition to that, similarly to the GDPR, the PIPL defines *processing* as "personal information collection, storage, use…transmission, provision,

disclosure, deletion, etc" (PIPL, Article 4). Nevertheless, this definition has a narrower exemplifying category when compared to the GDPR's.

Altogether, both the CCPA and PIPL term *personal data* slightly different and have a narrower categorization of *processing* compared to the GDPR; the CCPA includes extra-personal data and the PIPL emphasizes the fact that anonymized data is not considered as personal data in their definitions of "personal information". Nevertheless, despite such differences, it can be claimed that the definitions of both *personal data* and *processing* essentially constitute the same in all three jurisdictions.

## 4.3 Dimension 3: Data Subject Rights

Another important metric by which the GDPR's impact can be evaluated is *data subject rights*. To begin with, from the GDPR's eleven chapters, one (3) solely constitutes the rights of individuals on data processing by corporations. Roughly summarized, the GDPR presents seven rights for data subjects: the right to access data, to rectify data, to erase data (or "the right to be forgotten"), to data portability, to objection, to restrict processing and to resist profiling (Hoofnagle et al., 2019, p. 89). First, the right "to access" data grants individuals access to information about the categories of personal data, where their data was obtained, the processing purpose, the recipients of the data and the storage period (GDPR, Article 15.1). Second, the right "to rectify" allows data subjects to rectify inaccurate information concerning him or her (GDPR, Article 16). Third, the right "to erase" allows data subjects to erase their data when unlawfully processed or no longer necessary (GDPR, Article 17). Fourth, the right "to portability" increases the individuals' control by granting them the ability to transport their data from one platform to another (GDPR, Article 20.2). Fifth, the right "to object" allows data subjects to object to the processing of their data by corporations (GDPR, Article 21.1). Sixth, the right "to restrict" allows individuals to stop the processing of their data on the grounds of inaccuracy, unlawfulness and objection (GDPR, Article 18.1). Last but not least, the right "to resist" regulates profiling and computerized or automated processing of a natural person's data.

Following that, according to de la Torre (2018), some of these features are common to most "data protection frameworks around the world", and can also be found under the CCPA and PIPL. For instance, the CCPA presents six rights to data subjects residing in California: the right to know, to delete, to opt-out, to non-discrimination, and added most recently, the rights to correct and to limit (Bonta, 2023). In that case, the overall rights align with the GDPR; For example, the rights "to delete" and "to correct" are equivalent to the GDPR's rights "to erase" and "to rectify", respectively. Regarding the CCPA's right "to know", however, although generally similar to the GDPR's right "to access", it includes the disclosure of data sold to third-parties (Bonta, 2023). As opposed to the GDPR, the CCPA allows businesses to sell and disclose personal data, although it provides data subjects with the right "to opt-out the selling of their data" (de la Torre, 2018). In GDPR terms, the right to "opt-out" would be compared to the right "to restrict", and perhaps "to object". Lastly, similar to the GDPR, the CCPA also ensures data subjects with the right "to non-discrimination" for exercising their rights - although it emphasizes it more explicitly than the GDPR (de la Torre, 2018).

In terms of the PIPL, the law mostly aligns with the GDPR with regard to personal data rights as well. The PIPL presents nine rights to data subjects: the right to information, to

access, to rectify, to erase, to object and to restrict, to data portability, to profiling, to withdraw and to complain (PIPL, Articles 44-50). Even though some of those rights take a different form under the GDPR, they express the same purpose (Ke et.al, 2021). Nevertheless, according to Ke et.al (2021), the PIPL differs in that it does not include "a more precise GDPR language addressing such rights", and it also lacks a better-defined restrictions and exemptions section.

Overall, even though the CCPA and PIPL lack or contain extra legal characteristics when compared with the GDPR, the three jurisdictions empower individuals with similar fundamental rights in regard to information, accession, erasure, and withdrawal of consent (Calzada, 2022, p. 1140).

## 4.4 Dimension 4: Enforcement & Penalties

Finally, the ways by which each jurisdiction enforces its law on entities that trespass their obligations as data handlers, also give us a different perspective on the GDPR's influence. Under the GDPR, such enforcement of compliance is mostly emphasized through two mechanisms: Data Protection Authorities (DPAs) and penalties. To begin with, the GDPR strengthens supervisory independence through Data Protection Authorities. DPAs "supervise, through investigative and corrective powers, the application of data protection law" and, for that reason "there is one in each EU member state" (European Commission, n.d.-c). In case DPAs encounter GDPR violations, in addition to remedies and corrective powers to adjust compliance, *administrative fines* are triggered (GDPR, 2016). In that matter, there are two levels of fines based on the seriousness of the violation. Less serious violations shall be subject to administrative fines of up to ten million euros, or up to 2% of the total worldwide annual (net) turnover of the preceding financial year, whichever is higher (GDPR, Article 83.4). Whereas, more serious violations, shall trigger administrative fines up to 20 million euros, or up to 4% of the total worldwide annual (net) turnover of the preceding financial year, whichever is higher (GDPR, Article 83.5).

Similar to the GDPR, the CCPA designates a governmental body with enforcement jurisdiction: the California Attorney General's Office (de la Torre, 2018). In case such authority encounters CCPA violations, civil penalties are also triggered. Nevertheless, when compared with the GDPR, such fines/penalties can be considered less effective. Administrative fines, under the CCPA, may reach only up 2,500 USD for every unintentional violation and up to 7,500 USD for every intentional violation (Cal. Civ. Code, §1798.155 (a)).

Unlike the GDPR and CCPA, the PIPL does not designate supervisory tasks to a unified authority, but it rather grants this role to multiple governmental departments, such as the Cyberspace Administration of China (CAC), the Ministry of Public Security and the State Administration for Market Regulation (Wang, 2022). In regards to administrative penalties, the Regulation imposes fines between 100,000 and 1 million Yuan (~ 14,500 and 145,000 USD) in case corrections of such violations are denied by handlers; while, the person responsible for the breach is to be fined between 10,000 and 100,000 Yuan (~ 1,450 and 14,500 USD) (PIPL, Article 66). In case of more serious violations, the PIPL shall trigger administrative fines up to 50 million Yuan (~ 7 million USD), or up to 5% of the company's annual revenue (PIPL, Article 66), therefore, the fine in case of serious breaches is potentially higher under the PIPL when compared to the GDPR.

Altogether, the CCPA and PIPL impose less strict fines on companies that violate their respective jurisdictions (with the exception of PIPL's fine for serious violations) as opposed to the GDPR; and PIPL acquires multiple supervisory authorities in contrast to both the GDPR and CCPA which empower a unified supervisory authority. Nevertheless, the three legislations similarly acquire supervisory authorities and implement administrative fines in case of violations.

In short, this section makes clear that the GDPR has had a certain degree of normative influence on the CCPA and PIPL. Based on the comparison of the four dimensions above, it is possible to take the following general conclusion: the GDPR, CCPA, and PIPL are similar in the overall conduct of their respective legislations. Therefore, the key characteristics that constitute the GDPR can also be found under the CCPA and PIPL: (1) all three legislations have extraterritorial applicability, (2) the three legislations define the terms 'personal data' and 'processing' in a conceptually similar way, (3) all three legislations provide 'data subjects' with fundamental rights regarding their personal information, and (4) they all obtain supervisory authorities and enact administrative penalties based on the seriousness of the infraction.

Individually, they naturally contain specific elements that differentiate one from another: (1) unlike the GDPR and PIPL, the CCPA does not apply to entities that do not "do business" in California even if data is being processed; (2) the CCPA and PIPL have a narrower definition of *processing* when compared to the GDPR and individually add household data (CCPA) and emphasize anonymous data as not being personal data (PIPL) in their definition of *personal information*; (3) the CCPA provides a right to opt-out and emphasizes the right to non-discrimination, and the PIPL lacks a more detailed language and exceptions section when compared to the GDPR; and lastly, (4) while the GDPR and CCPA have a unitary supervisory authority, PIPL has multiple, and while the GDPR and PIPL trigger stricter fines, the CCPA opts for lighter ones.

Understandably, those individualities allow the U.S. and China to flourish their own interests regarding data privacy through a looser or stricter standpoint. Nevertheless, the foundational influence that the GDPR has had on both jurisdictions allows the EU to indirectly export its norms (NPE) through its regulatory standards (Brussels Effect), and consequently, further its influence on the global digital environment.

# 5 Conclusion

All in all, the European Union has clearly influenced the American CCPA and the Chinese PIPL through its GDPR. Therefore, in answering the research question of this thesis: how and to what extent, this paper has arrived at the following conclusions and limitations. First, the way by which the GDPR influences the CCPA and PIPL is through its core regulatory features. Therefore, in comparing the three legislations simultaneously, it is evident that the State of California and China implemented the structural foundations underlying the GDPR into their own data protection regulations, particularly, in regard to territorial scope, key terminology, data subject rights and implementation and penalties (as conclusively shown in greater detail under section 4.4).

Second, the EU's privacy regulation has influenced the other two regulations to the extent that both the U.S. and China find it to be beneficial to their internal systems. On the one hand, America's private-optimized system allows companies to have a say in America's regulatory agenda. Therefore, California's decision to align its jurisdiction with the GDPR has to a great degree to do with the pressure and lobbying from American multinational companies to facilitate their compliance. On the other hand, China's public-optimized system grants the Chinese government with a rather monopolized ability to set the regulatory agenda. Thus, China's decision to align its national law on data privacy with the EU's GDPR has rather been greatly incentivized by the government's strive for social control and protection from possible foreign threats. Appropriately, these characteristic alignment factors parallel with the countries' desire to set their own data-privacy jurisdictions as global standards. On that account, this thesis concludes that the Americans and Chinese have added, deleted, maintained or modified the GDPR's policy content in accordance with their internal systems and normative expectations.

Third and last conclusion, in regard to the GDPR's normative influence, although it is pretty clear that Bradford's Brussels Effect concept has a high degree of applicability to the findings of this thesis, it is not so clear the extent to which concrete conclusions can be taken as for Manners' NPE concept. The Brussels Effect is clearly evident, for example, through the non-divisibility preference by American companies, the Chinese and American desire to have access to the EU's profitable market and the EU's clear regulatory capacity to influence both the CCPA and PIPL through the GDPR ("de jure" Brussels Effect). Meanwhile, the NPE is the biggest limitation encountered in this thesis. Although this paper notes that the norms and values of the European project are essentially perpetuated through the legal and institutional standards set by the GDPR, it is difficult to access whether such normative influence has successfully been translated to the American and Chinese' very own norms and values when those countries adopted a GDPR-like legislation. As a result, this thesis cannot positively and conclusively state that the NPE was successfully achieved, thus, creating future and further research opportunities.

Nevertheless, this thesis can affirmatively conclude that the GDPR has undeniably served as a blueprint for both the CCPA and PIPL in a normative manner.

# 6 Bibliography


Allison, G. (2017). China vs. America: Managing the Next Clash of Civilizations. *Foreign Affairs*, *96*(5), 80–89. http://www.jstor.org/stable/44821871

Amuso, V., Poletti, G. & Montibello, D. (2019). The Digital Economy: Opportunities and Challenges. *Global Policy*, *11*(1), 124-127.

Bendiek, A. & Stuerzer, I. (2023). The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate. *DISO*, *2*(5), 1-25.

Bonta, B. (2023, May 1). *California Consumer Privacy Act (CCPA)*. State of California Department of Justice Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, *107*(1), 1-68.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Bygrave, L. A. (2021). The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanisms and Prospects. *Computer Law & Security Review*, *40*, 1-13.

California Civil Code (2018). Information Practices Act of 1977 - Code of Civil Procedure § 1798. State of California. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798&lawCode=CIV

Calzada, I. (2022). Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*, 1129-1150.

Custers, B. & Malgieri, G. (2022). Priceless Data: Why the EU Fundamental Right to Data Protection is at Odds with Trade in Personal Data. *Computer Law & Security Review*, *45*, 1-11.

Daniel, N., F. (2022). *EU Data Governance: Preserving Global Privacy in the Age of Surveillance*. Johns Hopkins University (Doctoral Dissertation). https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/67940/DANIEL-DOCTORALTHESIS-2022.pdf?sequence=1&isAllowed=y

De La Torre, L. (2018, July 31). *GDPR Matchup: The California Consumer Privacy Act 2018*. IAPP. https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/

Diez, T. & Manners, I. (2007). Reflecting on Normative Power Europe. In F. Berenskoetter & M. J. Williams (Eds.), *Power in World Politics* (1st ed., pp. 173-188). Routledge.

Enli, S., G. (2010). *Comparative Analysis and Case Studies*. University of Oslo. https://www.uio.no/studier/emner/hf/imk/MEVIT4800/h10/Method_4800_9.11.10.pdf

European Commission (n.d.-a). *Adequacy Decisions*. Author. Adequacy decisions

European Commission (n.d.-b). *EU Trade Relations with China*. Author. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en

European Commission (n.d.-c). *What are Data Protection Authorities (DPAs)?*. Author. https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

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

European Union Agency for Fundamental Rights (FRA) (2007). *EU Charter of Fundamental Rights: Article 8 - Protection of Personal Data*. Official Journal of the European Union (C 303/17). https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data

European Union Agency for Fundamental Rights (FRA) (n.d.). *What are Fundamental Rights?*. Author. https://fra.europa.eu/en/about-fundamental-rights

Forsberg, T. (2011). Normative Power Europe, Once Again: A Conceptual Analysis of an Ideal Type. *JCMS*, *49*(6), 1183-1204.

General Data Protection Regulation (GDPR) (2016). *Legislation*. Official Journal of the European Union (L 119/1). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

Gorostiza, A. & McMillan, J. (2022). An Analysis of Privacy-Impacting Regulatory Efforts and Their Effect on Service Providers and Individuals. *ACM*, 1-7.

Gunst, S. (2021). The Brussels Effect: How the GDPR Conquered Silicon Valley. *European Foreign Affairs Review*, *26*(3), 437-458.

Gur, B., A. (2020). The Normative Power of the EU: A Case Study of Data Protection Laws of Turkey. *International Data Privacy Law*, *10*(4), 314-329.

Hadjiyianni, I. (2021). The European Union as a Global Regulatory Power. *Oxford Journal of Legal Studies*, *41*(1), 243-264.

Hoofnagle, C., J., Sloot, B., V., D. & Borgesius, F., Z. (2019). The European Union General Data Protection Regulation: What it is and What it means. *Information and Communication Technology Law*, *28*(1), 65-98.

International Monetary Fund (IMF) (2018). *Measuring the Digital Economy*. Author. https://doi.org/10.5089/9781498307369.007

Jehl, L. & Friel, A. (2018). *CCPA and GDPR Comparison Chart*. Practical Law. https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf

Ke, X., Liu, V., Luo, Y. & Yu, Z. (2021, August 24). *Analyzing China's PIPL and How it compares to the EU's GDPR*. IAPP. https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/

Luo, D. & Wang, Y. (2022, November). *China - Data Protection Overview*. DataGuidance. https://www.dataguidance.com/notes/china-data-protection-overview

Manners, I. (2002). Normative Power Europe: A Contradiction in Terms?. *Journal of Common Market Studies*, *40*(2), 235-258.

Molnár, P. (2021, December 20). *Comparison of the New Chinese Personal Data Protection Law (PIPL) with GDPR and CCPA*. KRE-DIt. https://www.kre-dit.hu/tanulmanyok/peter-molnar-comparison-of-the-new-chinese-personal-data-protection-law-pipl-with-gdpr-and-ccpa/

Moreira, H. (2023). *Governing Knowledge and Technology: Technological Pressure for Convergence in EU, California and China Data Protection Regulation*. CIES. https://doi.org/10.31235/osf.io/v6uf3

Noureddine, R. (2016, November 24). *Critically Assess and Analyse the Notion that the EU is a Normative Power*. EEAS.

Personal Information Protection Law (PIPL) (2021, August 20). *Translation: Personal Information Protection Law of the People's Republic of China - Effective Nov. 1,2021* (R. Creemers & G. Webster, Trans.). Standford University.

Reid, R. (2022). Data Privacy. In R. Reid (Ed.), *Practical CockroachDB* (1st ed., pp. 123-138). Apress.

Savaroskaya, E. (2015). The Concept of the European Union's Normative Power. *Baltic Region*, *7*(4), 66-76.

Sjursen, H. (2006). What Kind of Power?. *Journal of European Public Policy*, *13*(2), 169-181.

Skolimowska, A. (2015). The European Union as a "Normative Power" in International Relations: Theoretical and Empirical Challenges. *Yearbook of Polish European Studies*, *18*, 111-131.

The White House (2015, September 25). *FACT SHEET: U.S.-China Economic Relations*. Author. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-us-china-economic-relations

Todt, K. E. (2019). Data Privacy and Protection: What Businesses Should Do. *The Cyber Defense Review*, *4*(2), 39–46. https://www.jstor.org/stable/26843891

Treaty on European Union (TEU) (2008). Article 21(1). Official Journal of the European Union (2008/C 115/01).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3AC2008%2F115%2F01

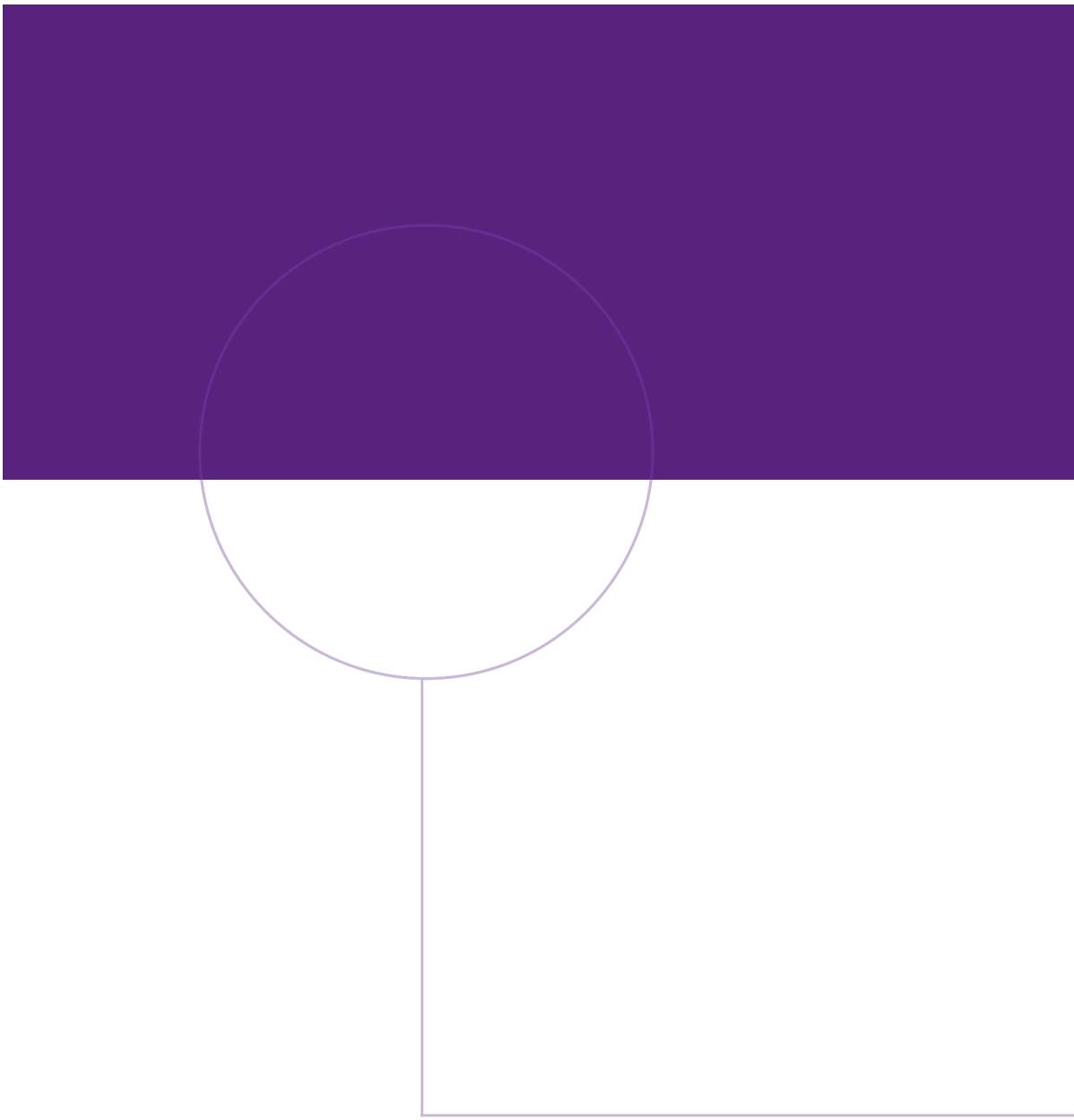
Treaty on the Functioning of the European Union (TFEU) (2008). Article 169.Official Journal of the European Union (2008/C 115/01). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3AC2008%2F115%2F01

Victor, J. M. (2013). The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. *The Yale Law Journal*, *123*(2), 513–528. http://www.jstor.org/stable/23744289

Wang, I. (2022, March 2). *Top 5 Operational Impacts of China's PIPL - Part 4: Penalties and Enforcement Mechanisms*. IAPP. https://iapp.org/news/a/top-5-operational-impacts-of-chinas-pipl-part-4-penalties-and-enforcement-mechanisms/

Yin, R. K. (2017). *Case Study Research Applications: Design and Methods*. Sage.

Zuckerberg, M. (2019, March 30). *Mark Zuckerberg: The Internet Needs New Rules - Let's Start in These Four Areas*. The Washington Post. Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas. - The Washington Post



NTNU

Norwegian University of
Science and Technology