Data Protection as a Fundamental Right: The European General Data Protection Regulation and Its Exterritorial Application in China

Bo Zhao
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg, Netherlands

Weiquan Chen
Tilburg University, Tilburg, Netherlands

The right to data protection is a fundamental right recognized by the EU Charter of Fundamental Rights (Art. 8) and constitutional law of most Member States, as well as ECJ case law. As a leading legislation, the European General Data Protection Regulation (GDPR) concretizes and materializes the right by means of granting a constellation of specific rights to data subjects, and establishes stringent law compliance mechanisms for their realization. Further, the GDPR claims a wide extraterritorial jurisdiction to protect all data subjects on the EU territory – regardless of their nationalities, when their personal data are transferred to third countries outside the EU. Apparently, many controllers and processors processing their data on Chinese territory will be directly influenced and may encounter law breaches with negative consequences that may lead to conflict of law and jurisdiction. This short article will first discuss data protection as a fundamental right under the EU law and how GDPR can protect that right with different instruments. Then, it will analyze in detail GDPR’s exterritorial application to controllers and processors in China and their related data protection roles and duties under various processing circumstances, as well as the different impacts on their data processing operations for law compliance and the potential incurred costs.

Keywords: data protection, GDPR, exterritorial implementation, China, fundamental right

Introduction

In EU, the right to data protection is a fundamental right recognized by the Charter of Fundamental Rights of the European Union (Article 8, hereafter the Charter) and constitutional laws of many Member States (Molnar-Gabor, 2016), as well as the case law of European Court of Justice (hereafter ECJ). The exercise of this right...
right and the enforcement of the incurred duties and responsibilities of data controllers and processors that process various personal data of EU residents, become critically important in the context of increasing digitalization and connectedness of our globalized economy and community. As a leading, comprehensive legislation in the field, the European General Data Protection Regulation (hereafter GDPR) aims to not only facilitate data flows within the EU, but also concretizes and materializes, for the first time in a systematical way, this right by means of granting a group of specific rights (to data subjects) and protecting them through establishing a strict law implementation mechanism. This includes the rights to access, information, objection, data portability, explicit consent (and withdrawal of consent), data rectification, data erasure (the right to be forgotten), remedy, etc. More importantly, GDPR claims protection of all data subjects that reside in the EU, regardless of their nationalities, and regulates cross-border data transfers towards non-EU countries, thus being applicable to the controllers and processors that are not on EU territory, but process personal data of natural persons in EU. There have been, however, rising doubts over the protection of the fundamental right in the context of exterritorial application of the related GDPR rules.

Apparently, a large number of data controllers and processors in China will fall under the scope of GDPR when they process EU resident’s personal data. Their business activities will be directly influenced and may largely risk potential law breach in case they may not follow GDPR’s data protection requirements for various reasons. This is an issue with rising significance that deserves both side’s attention. First, China now is EU’s second largest trade partner and EU is China’s largest trade partner. Thus, there is a huge amount of cross-border data transfers considering their still growing economic, societal, and political connections. Theoretically speaking, they may encounter negative consequences including administrative fines or other sanctions, in addition to litigations initiated by harmed data subjects in EU. This may lead to future conflict of law and jurisdiction between China and EU Member States (hereafter MSs), causing potential diplomatic or political controversies amidst rising global scrutiny over Chinese ICT products regarding national security and business espionage.

Second, cross-border data transfers to China can happen in unexpected ways, bringing up greater data protection concerns at global level. For instance, it is reported recently that Facebook has data sharing partnerships with at least four Chinese electronic companies dated back to 2010, offering broad private access to user data to Huawei, Lenovo, Oppo, and TCL without user’s consent. Such data sharing allows the Chinese partners to retrieve detailed information on both device users and all of their friends, including religious and political leanings, work and education history, and relationship status. Similar data sharing also includes other manufacturers, including Amazon, Apple, BlackBerry, and Samsung (Liao, 2018; LaForgia & Dance, 2018). A fair assumption is that the same would also happen to EU data subjects whose data can be accessed and analyzed.

---

1 Recital 10: “to remove the obstacles to flows of personal data within the Union”. The same rationale is also witnessed in the new EU Regulation on the free flow of non-personal data promulgated in Nov. 2018.
2 See European Commission’s introduction at: http://ec.europa.eu/trade/policy/countries-and-regions/countries/china/.
3 As recently seen in U.S. government’s attack against ZTE and Huawei. See Trump helps sanctioned Chinese phone maker after China delivers a big loan to a Trump project. Vox, https://www.vox.com/policy-and-politics/2018/5/15/17355202/trump-zte-indonesia-lido-city (last visited Jun 17, 2018).
4 The rising concern at this point is whether the shared data could have reached Chinese servers or been passed over to a third party, even though Facebook insisted that all the information from Huawei’s integrations was stored on the device, but not on Huawei’s servers.
when they use Huawei’s devices and other Chinese digital products as third party service providers.

Third, legally speaking, as a fundamental right, it is of a vital concern about to which extent the EU may protect this right outside the EU territory, when enforcing national law exterritorially is an issue more of political and diplomatic nature than legal. The critical issue is the enforcement jurisdiction of the GDPR regarding whether its data protection rules and future court decisions can be complied with by Chinese data controllers and processors on Chinese territory (Berman, 2018). Their non-compliance of GDPR rules may pose a big threat to GDPR’s extraterritorial application in specific and the law’s legitimacy in general. Last, the implementation of GDPR’s data protection rules may have other indirect impacts on both private and public sectors in China in the sense that China may need to consider seriously to level up her data protection in multiple ways in order to help with her global economic expansion and influence in the ICT sector that has been largely hindered by lack of general trust on foreign market.

Thus, this short paper is meant to explore to which extent data protection as a fundamental right can be secured in China under the new cross-border data protection framework that has been established by GDPR. Section two will first briefly introduce the right to data protection as a fundamental right in the EU law framework. Section three will then explain how the GDPR has contextualized and concretized the fundamental right by setting up different legal constructions. Section four will discuss in detail GDPR’s extraterritorial scope under Article 3 and its legal impacts on controllers and processors established in China but processing EU resident’s data, and their potential reactions to the related obligations and requirements. It will in particular analyze the problems and difficulties in GDPR’s extraterritorial application in China’s special legal context. The last section intends to provide a much broader scenario of the situation, as well as a few temporary solutions to bridge the existing loophole.

**Data Protection as a Fundamental Right**

Article 8 of the Charter of Fundamental Rights of the European Union (the Charter) prescribes: “Everyone has the right to the protection of personal data concerning him or her” and “Such data must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”. Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provides that everyone has the right to the protection of personal data concerning him or her. The creation of this positive right, independent from the right of privacy, is a leading feature of the EU legal order and has promoted data protection to the highest status of fundamental right in EU law, although whether this new right is fundamental or not in other jurisdictions, or even within the EU, can be more or less debated (Sloot, 2017). In the EU law context, the term “fundamental rights” is consistently referred to, rather than human rights and constitutional rights (Sloot, 2017, p. 5). However, it shall be noticed that the Charter is different from traditional human rights instruments,

---

5 Enforcement jurisdiction means the power to induce or compel compliance or to punish noncompliance with the law. It is a matter of international law principle that a state may not exercise its power in any form in the territory of another state failing the existence of a permissive rule to the country.

6 See in general, Bart van de Sloot’s arguments against the legal status of the right to data protection as a fundamental (human right), including: (a) most aspects of data protection do not seem to find the underlying idea of human or fundamental rights; (b) one of the dual aims of data protection rules is to facilitate data processing activities and ensure that they are conducted in a fair and adequate manner; and (c) both the Data Protection Directive and the GDPR are akin to market regulation than traditional human rights instruments.
such as the European Convention of Human Rights, in a complex way, not as a free standing bill of rights with a universal scope; rather it applies to EU institutions and MSs only when they are implementing EU law (Mostert, Bredenoord, Slootb, & Delden, 2017).  

First, the right to data protection can find its root partly in the data protection rules of northern European countries, the Council of Europe’s Resolutions on data processing, and partially in the US and the realization of the Fair Information Practices (FIPs) (Sloot, 2017; Fuster & Gellert, 2012). At the earlier stage, EU data protection legislation is oriented to market regulation and facilitation of the free flow of information; and the data protection rules primarily aim at safeguarding the fairness and carefulness of data processing activities, while the Council of Europe was handling the protection of human rights (Sloot, 2017). While the EU started to address data protection, the original mandate to regulate data protection was found in market regulation, and this right was in the beginning strongly connected to the right to privacy, as such well-observed in the Data Protection Directive 95/46/EC (hereafter the Directive) (Sloot, 2017).

Second, the right to data protection has been disconnected from privacy protection at the final version of the drafting of GDPR that at last contains no reference to the right to privacy. Article 1(2) states: “This regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”. Unlike the Directive, GDPR finds its legal base on the right to data protection as specified in Article 16 of the Treaty on the Functioning of the European Union. This Article prescribes that everyone has the right to the protection of personal data concerning them and the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by MSs when carrying out activities which fall within the scope of the Union law and the rules relating to the free movement of such data. Also, the disconnection of the right to data protection from the right to privacy protection can be found in Article 8 of the Charter of Fundamental Rights which was adopted in 2000 and came into force in 2009. It is clear that data protection has been fully disconnected from the right to privacy at least in terms of terminology (Sloot, 2017).

Third, consequently, the right to data protection is now protected at the highest level both as a fundamental right and the EU has an explicit mandate to regulate the field of data protection (Sloot, 2017). The European Court of Justice (ECJ) has retrospectively interpreted the Data Protection Directive as the application of Article 8 of the EU Charter (Sloot, 2017), in the verdicts of Schrems, Google Spain, and Coty as a common approach (Sloot, 2017). This is in contrast to ECJ’s earlier reluctance to refer to the right to data protection, as it suddenly made a direct quotation in Promusicae in 2008. The ECJ started to address the issue of data protection on many occasions (Fuster & Gellert, 2012), especially from the Eifert judgment in 2010 (Bonnici, 2014). It is in the joined Cases Voker and Markus Schecke GBR and Hartmut Eifert v. Land Hessen judged in 2010 that the ECJ explicitly mentioned the protection of personal data as a fundamental right established by Article 8(1) of the

---

7 The EU and MS law should be in accordance with the Charter as a minimum requirement and a provision in EU law and MS law could not be applicable when in conflict with the Charter, since the Charter is to guide the implementation and interpretation of EU law.
8 But the EU’s approach as the regulator of a common EU market still strongly connected with privacy protection as seen in the Directive 95/46/EC.
9 In Coty, the Court argued that the whole directive shall be taken as an implementation of Article 8 of the EU Charter.
10 Promusicae v. Telefónica de España C-275/06.
DATA PROTECTION AS A FUNDAMENTAL RIGHT

Charter and connected the right with the right to respect for private life in Article 7 of the Charter (Fuster & Gellert, 2012). In Eugen Schmidberger, the Court ruled that the right to data protection is not an absolute right, but shall be considered in the context of its function in society. In the 2011 Deutsche Telekom, the Court clearly announced that the Directive’s aim is to ensure the observance of the right to the protection of personal data, departing from its old assertion in favour of the right to privacy. Since this case, the Court:

reverberated the construction of the right to personal data protection according to which the first paragraph of Article 8 of the Charter would describe the right itself, whereas the first indent of the second paragraph would define the conditions under which processing of personal data can be authorised (§ 52). (Fuster & Gellert, 2012, p. 78)

Although the right to data protection in EU is not absolute but with certain limitations (Bonnici, 2014, p. 17), it has been, as a fundamental right, undergoing a fast extension both through ECJ’s recent decisions and legislative measures (mainly EU secondary legislation) (Brkan, 2016). As for the right itself, it is not only the case that the material scope of the right is expanding, but also the territorial scope reaches far outside the EU at least on paper. Compared to many other fundamental rights, data protection is also gaining importance over other rights or interests, such as public security, freedom of information, and economic interests of the controller (Brkan, 2016). As a fundamental right, it shall apply to all natural persons in the EU (regardless of their nationality), all data processing operations (except outside the EU law scope) and all personal data (whether identified or identifiable). The practical significance of the new right lies in the establishment of a robust legal framework to tackle many practical challenges, and the creation of this new right adds normative force to data subject’s claim in that “the framing of data protection as a right appears to have imposed much greater obligations on private actors than most other human rights” (McDermott, 2017)

Last, although data protection has been generally accepted as a fundamental right or treated as a sub-set of or as equivalent to human rights (Sloot, 2017, pp. 18-19), an essential problem remains unsolved: What is the right to data protection, or more specific, What does the right to persona data actually consist of? (Bonnici, 2014, p. 133). Hondius (1980) defined the right to data protection broadly as “the protection of the rights, freedoms and essential interests of persons vis-à-vis the processing of personal information relating to them, particular when computers aid in the processing procedure” (pp. 87, 89). Rodotà (2009) approached this right as the endpoint of a long evolutionary process experienced by the privacy concept that “from its original definition as the right to be left alone, up to the right to keep control over one’s information and determine how one’s private sphere is to be built up”. However, there has been no general agreement on what constitutes the right to data protection, albeit most authors define it either from the perspective of privacy protection, or from these principles found in the Council of Europe Convention 108 or the Directive 95/46/EC (Bonnici, 2014, p. 133). As Gutwirth, Poulet, de

---

11 Eugen Schmidberger, Internationale Transporte und Planzüge v. Republik Österreich, Case C-112/00, at para. 80.
12 Deutsche Telekom AG v Bundesrepublik Deutschland Case C-543/09, at para. 50.
13 According to Bonnici, in general, limited by its societal function, positive delimitations of the right as formulated in the Charter, limitations imposed by Article 52 of the Charter (consent, respect of the essence of the fundamental rights and freedoms and proportionate), the connection between Article 7 right to privacy and Article 8, detailed provisions in current data protection secondary legislation and future data protection regulation framework.
14 For instance, as Purtova rightly pointed out (Purtova, 2017), the definitions of personal data and data processing of the GDPR may have include almost all processing connecting to (in most cases) personal data in today’s data driven economy and community. For a criticism of the broad definition of personal data.
15 See Bart’s discussion of the fundamentalisation of data protection (In particular Section 1.3).
Hert, de Terwangne, and Nouwt (2009) commented, “data protection is a catch-all term for a series of ideas with regard to the processing of personal data”.

**GDPR: Contextualizing Data Protection and Expanding Exterritorial Claim**

Responding to the definitional puzzle, the right to data protection, as a fundamental right, can be better approached as an umbrella right that consists of a set of concrete rights or entitlements for realization and materialization. As Bonnici (2014) pointed out, the (data protection) rules are not only conferred on the data subjects, but also on independent authorities entrusted with ensuring that the rights of data subjects are protected (p. 134). First, this independent right has been underpinned by a series of fundamental values and interests endorsed by different MSs, including privacy, autonomy, transparency and non-discrimination (McDermott, 2017, 26), as well as dignity (European Data Protection Supervisor, 2015). This is similar to the right to privacy that does not have a single, concrete core (Solove, 2008), but a constellation of multiple interests, freedoms, and legal entitlements (Benn, 2017). Second, as an umbrella right, the right to data protection consists of multiple specific rights protecting personal data in the course of different data processing operations. The right to data protection certainly is not a single entitlement under law, but a cluster of entitlements and interests recognized and endorsed under the EU law.

In this context, the GDPR, as a secondary legislation, has played a vital role in the construction of the right to data protection, by providing, among others, a rich list of the relevant concrete rights for its realization and concretization. Many of such rights have previously been delineated in other EU legal acts and in different forms, including the Charter (mentioning consent in Article 8), especially the European Data Protection Directive (explicitly explaining the rights to information, access, objection, erasure, rectification, and remedy). But, for the first time, all these rights are formally formulated and recognized as positive legal rights in a EU Regulation that is directly enforceable on EU territory and backed up by a strong right protection mechanism. At the EU level, this is taken as the concretization of European constitutional law **vertically** against public controllers and processors and **horizontally** against private controllers and processors (Leczykiewicz, 2013).

First, under the GDPR, each specific right, e.g., the rights to access, rectification, erase, rejection, and consent (and withdrawal of consent), has clear corresponding duties imposed on controllers and processors to assist data subjects to exercise these rights. Second, there are specified obligations for controllers and processors to process data lawfully and fairly, including obligations to inform/notify data breach, cooperate with competent supervisory authorities and other data protection authorities, keep records of processing, provide necessary information to data subjects, data security, etc. For further data transfers to a third country outside the EU, there are detailed requirements for lawful transfers to provide data protection outside the EU jurisdiction, on the grounds of: (a) adequacy decision; (b) appropriate protection; and (c) derogations under specific circumstances.

---

16 As well explained by the European Data Protection Supervisor: “the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing”.

17 As Solove pointed out: “It seems as though everybody is talking about privacy, but it is not clear exactly what they are talking about”.

18 The umbrella right to privacy extends to other claims besides the claims not to be watched, listened to or reported upon without leave, and not to have public attention focused upon one uninvited.
Third, the GDPR has established a strong law enforcement mechanism, characterized by independent supervisory authorities of MSs with considerable regulatory powers, and the consistency mechanism to ensure the coherent law enforcement across EU, with the European Data Protection Board (EDPB) as the overseeing authority at the EU level.\footnote{Hereafter the Board, the successor of the previous Article 29 Working Party established under Article of the Directive 95/46/EC.} Fourth, the GDPR also adopts other flexible legal instruments of soft law or self-or-co-regulation nature to streamline law compliance, in order to adjust to complex business practices, in addition to hard laws including data subject compliant mechanism, administrative sanctions, and various remedies in case of law breach. This includes measures of data protection certification mechanisms, Codes of Conduct (COCs) and Binding Corporate Rules (BCRs).

Further, to safeguard the right to data protection, a striking feature of the GDPR is the high administrative penalties imposed on law violators and the strong powers of the data protection supervisory bodies for law enforcement across the EU. EU supervisory authorities can directly use their investigative powers to investigate law breaches (either upon or not upon data subject’s request) and correct wrong acts of controllers pursuant to Article 58.\footnote{See the details of investigative and corrective powers in Article 58 of GDPR.} They can order processors and controllers to suspend or/and stop data processing, provide information to data subjects upon request, provide necessary information needed for their investigation, etc. In addition, data protection authorities may impose a fine up to max. €20 million or 4% of global annual turnover (whichever is higher). Data subjects may lodge a proceeding against controllers to claim damages in accordance with Article 79. Controllers or processors may also be subject to other penalties laid down by MS laws, if not regulated by the GDPR (Article 84).\footnote{Article 84 of GDPR.} In order to provide the best possible remedy for data subjects, controllers, joint-controllers,\footnote{Joint controllers are two or more controllers that jointly determine the ends and means of data processing (Article 26).} and processors shall first pay all compensation for the damages suffered by a data subject and then can claim their due part(s) from other parties; unless they can prove that they are not in any way responsible for the event giving rise to the damage (Article 82).

A last strong feature of the right to data protection under the GDPR is the nationality-blind protection that protects all natural persons in the EU regardless of their nationality, and the broad extraterritorial application that it aims to maintain EU’s high level of personal data protection outside EU territory.

The nationality-blind protection is an advantage of the fundamental right that represents the aspirational aspect of GDPR (Solove, 2018).\footnote{As Solove said, “It’s an aspirational law”.} However, it is rather dubious at least to which extent GDPR’s generous promise of extraterritorial protection can be kept in complex business reality. The uncertainty and vagueness of the extraterritorial application of GDPR has led the EDPB’s recent publication of draft guidelines for public consultation, partially aiming to clarify or limit the wide territorial claim of Article 3 (Petrovici, 2018).\footnote{This article will consider the related opinions of this consultation paper because of EDPB’s authority on the matter and the expectation of merely minor changes in the last draft.} Despite GDPR’s good will, the hush reality is that EU law cannot protect EU citizen’s personal data in most important jurisdictions outside the EU. Multiple layers of conflict of law and jurisdiction are of ever growing concern in a globalized and digitalized world.

\textsuperscript{19} Hereafter the Board, the successor of the previous Article 29 Working Party established under Article of the Directive 95/46/EC.
\textsuperscript{20} See the details of investigative and corrective powers in Article 58 of GDPR.
\textsuperscript{21} Article 84 of GDPR.
\textsuperscript{22} Joint controllers are two or more controllers that jointly determine the ends and means of data processing (Article 26).
\textsuperscript{23} As Solove said, “It’s an aspirational law”.
\textsuperscript{24} This article will consider the related opinions of this consultation paper because of EDPB’s authority on the matter and the expectation of merely minor changes in the last draft.
First, there are only a small number of countries on EU’s adequacy decision list with a limited number of jurisdictions covered. Further, as the home jurisdiction of most digital giants operating in EU, the U.S. has only been accepted as providing adequate protection limited to the scope of Privacy Shield Framework. But there are criticisms of the Privacy Shield Framework amidst constant litigations (Evans & Mercer, 2018), leading to the recent adaptation of the European Parliament resolution calling for the suspension of the EU-US Privacy Shield agreement (Privacy & Data Security Team, 2018). Another telling example is the protection of EU citizen’s personal data extraterritorially in China. As a rising global digital power, China has a number of digital products and services providers operating in EU including Huawei, Oppo, Wechat, Alibaba, etc. (and other non-digital ones) that will unavoidably transfer personal data from EU to China for processing (Savov, 2019). This is especially the case when China is EU’s second largest trade partner and EU is China’s the largest trade partner. In view of China’s still growing bilateral connections and relationships with EU in economy, diplomacy, education, research, and culture, there will be more data transfers from EU to China in the near future. Whether EU residents’ personal data could be protected in China and to which extent is a very important issue with respect to GDPR’s extraterritorial application.

The following section will illustrate some of the difficulties and realities of GDPR’s broad territorial application in China with regard to the right to data protection, when China on the whole still does not directly recognize and enforce foreign court decisions at this moment, and even in the seeable future for political-economic reasons. Thus, the high administrative sanctions and various remedies under GDPR would be problematic in terms of their enforceability outside EU. The following section will first discuss the various circumstances under which controllers and processors in China will directly be governed by GDPR when they process EU resident’s persona data in China meeting the onditions prescribed by Article 3, and the underlying strong rationales that they may follow or neglect related GDPR obligations. Then, the last section offers a short summary of GDPR’s impacts on data processing practices and a few feasible options to move forward.

**Legal Impacts and Potential Reactions**

Controller under GDPR (Article 4) means the natural or legal personal, public authority agency, or other body that alone or jointly with others determines the purposes and means of he processing of personal data; and processor means a natural or legal person, public authority, agency, or other body which proceses personal data on behalf of the controller. Data controllers and processors located in China can fall under the extraterritorial scope of the GDPR under Article 3, in case they offer goods or services (with or without payment) to natural persons in the EU, or monitor data subject’s behavior taking place in EU. Regarding data transfers to China,

---

25 With Japan recently added and an ongoing talk with South Korean, such decisions only include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and U.S. See https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countr ies_en.

26 This leads to the uncertain status of the bilateral arrangement, which may ends in protracted negotiations for modifications to or replacement for the agreement.

27 For instance, roughly one third of smartphone shipments in Europe in 2018 were from Chinese manufacturers with Huawei taking the the lead, ending up with more than 23 percent of the overall market in the final months of the year.

28 See China-Trade-European Commission, http://ec.europa.eu/trade/policy/countries-and-regions/countries/china/ (last visited Jun 18, 2018). On this point, the protection of EU citizen’s personal data in China, if compared with the US-EU controversy, is indeed a Bermuda, with nothing coming out.
GDPR will be binding on EU resident’s personal data that are transferred from EU to China and transferred further from China to other third countries (Petrovici, 2018, p. 19).

First of all, the most affected controllers and processors located in China will be these Chinese companies and institutions with certain establishments or setups in EU under Article 3(1). They will be directly governed by GDPR and other related EU data protection laws (including those of MS’s). GDPR does not define the concept of establishment for the purpose of Article 3. Recital 22 of the GDPR explains that establishment as the proxy for law application implies the effective and real exercise of activity through stable arrangements, and the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. To determine whether an entity has an establishment in a MS, the key factors are degree of stability of the arrangements and the effective exercise of activities in that MS in light of the specific nature of the economic activities and the provision of services concerned (Petrovici, 2018, p. 19). When processing of personal data carried out in the context of the activities of an establishment, the controller or processor will be subject to obligations.

Thus, the most influenced controllers and processors in China will include digital corporates, such as Huawei, Alibaba, Xiaomi, and Tengxun, and other business entities like the banks that are based in China and have offices, branches, or subsidiaries in EU. The threshold for stable arrangement is rather low in some circumstance here, meaning the presence of one single employee or agent may be sufficient to constitute a stable arrangement (Petrovici, 2018, p. 19). First, they may have employees or representatives in EU and need to collect or process personal data for management and business purposes. This will involve data transfers to China and processing special categories of personal data like health data, because these employers need to provide insurance and other social welfare to employees. More importantly, these companies also collect and process personal data in the contexts of their business activities from EU customers and consumers. The amount of collected data can be large, depending on their business scale (e.g., online social media or networking services, such as Wechat), and may also include special categories of personal data under the GDPR including biometric data and genetic data under Article 4. All these data can be further transferred back to their head offices in China for further processing, or to a third country in which they may have other establishments. They are the directly influenced companies that must comply with all GDPR obligations; otherwise, they may directly face administrative sanctions and litigations initiated by harmed data subjects who are influenced by their processing activities. In fact, these multinational institutions and corporates have sufficient resources to comply with GDPR at their best when they are deeply involved in, or willing to perform better on EU market.

Further, other controllers and processors in China that are captured under Article 3(1) may also include, for instance, Chinese traveling agencies or product producers that do not establish their own European offices or branches, but engage re-sellers or collaborators in EU to promote business. They may collect and process EU customer’s data in order to provide related services and products. In this respect, they can be (joint)-controllers or processors under GDPR, depending on their specific business roles and whether they can decide, independently or jointly, both the ends and means of data processing incurred in business operations. If they are not the dominating party in business cooperations, but merely follow orders from EU partners and thus cannot decide on

---

29 Article 3(3) will not fit into the context of this thesis when MS law applies by virtue of public international law.
both ends and means of processing, they are data processors that process data on behalf of EU partners. In this case, controllers in China will have full GDPR obligations to fulfil that are equal to EU controllers, while processors in China shall abide by the contract or other legal act following GDPR requirements (Article 28[3]). Mostly, they can be small-or-middle-sized enterprises (SMEs) that have less resource to fully comply with the incurred GDPR duties and requirements for lawful and fair processing (including data transfers to China) when they fall under the EU jurisdiction.

Under Article 3(1), the situation of some controllers and processors in China is a bit vague and tricky. They are the controllers and processors that are in China but operate websites or have online presence that can be treated as “establishment” under Article 3(1) and previous ECJ case law. In the famous Weltimmo, the European Court of Justice clarified the territorial scope of the Directive 95/46/EC by focusing on the concept of establishment. Among other stable arrangements, the Court pointed out that the running of one or several properties dealing websites concerning properties situated in Hungary, which are written in Hungarian and whose advertisements are subject to a fee after a period of one month, could be regarded as a real and effective activity, even a minimum one. In this context, one may argue that if Chinese controllers and processors do not have any form of physical establishment in the EU (such as offices, subsidiaries, or branches), but have some stable arrangements (such as running a business website in a MS language and targeting EU data subjects) in EU, they may fall under the definition of establishment and thus the territorial scope of GDPR. Though in this case, these Chinese controllers and processors may fall under Article 3(1), it is more the case that Article 3(2) will first apply to these controllers and processors and establishment is a less important factor in terms of legal relevance. But in any case, the notion of establishment is not without limit that a non-EU entity cannot be assumed to have an establishment in the Union merely because the undertaking’s website is accessible in the Union (Petrovici, 2018, p. 5). This type of controllers and processors in China can be both large and small sized entities and many of them can be Chinese corporates willing to extend their business to EU market via the Internet. Their GDPR compliance depends largely on their good wills, first because of their non-physical presence in EU and seond the non-application of foreign law on Chinese territory.

The second large category of controllers and processors in China that will be regulated and influenced by GDPR are those that do not have any establishment in EU, but process personal data of EU residents. Under Article 3(2), if their business operations involve the following activities, they will be regulated by the GDPR.

In the first instance, if Chinese entities offer goods or services to EU residents regardless with a payment or not, GDPR will apply to them. Goods and services include the offering of information society services defined in Article 1(1)(b) as any service normally provided for remuneration at a distance by electronic means and at the individual request for a recipient of services (Petrovici, 2018, p. 14). The evidential factors to clearly show the intention to provide such services and goods, under Recital 23 of the GDPR, include the use of a language or a currency generally used in one or more MSs with the possibility of ordering goods and services in that other language, or the mentioning of customers or users in the Union. For example, an online seller in China sell products (either hard device or software) to EU citizens, either via its own website(s) in an EU MS language or via other business online platforms (for instance Alibaba or Jingdong) that purposely target EU consumers with

---

30 See Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Judgment of 1 Oct. 2015, ECLI:EU:C:2015:639, at para 9, 29 & 33.
clear evidence. They will be controllers (or joint controllers) deciding on the purposes and means of data processing (or together with the platform service providers).\(^{31}\) This also includes the using of Chinese apps on smart phones (such as WeChat) by EU residents, which can be apps in Chinese or in a MS language, in that the Chinese app designers or (and) owners actually target services at EU residents on purpose (Petrovici, 2018, pp. 13-14),\(^{32}\) and process their data that are necessary for providing such services.\(^ {33}\) Another good example is the provision of cloud services to EU residents by a Chinese company (in China), such as Baidu that still has no business setup in EU at this moment, but processes EU resident’s personal data due to registration and various data uploading activities (Flint, 2017a; 2017b).\(^{34}\)

In such contexts, a classic case of the cross-border data transfers would be that a Chinese company (in China) acquires data from an EU controller or EU processor for processing. This company is either a joint-controller or processor, or a controller, and thus needs to follow GDPR requirements for legal and fair data processing as well as transferring data to China.\(^ {35}\) However, another practical circumstance would be that a Chinese data controller can directly collect personal data from EU residents itself, when the latter accesses and use their services host in China, or use their apps installed on digital devices, such as smart phones, desktops, tablets, or laptops. In this case, the controller’s direct collection of personal data from EU data subjects involves cross-border data transfers at least technically speaking. A further processing practice is that a Chinese controller or processor (then as a third party) may get data indirectly from another Chinese controller (which is still in China but with no establishment in EU), such as from Baidu (in case of cloud service) or Youdao (an online dictionary service providing cloud services on the condition of verified registration) for further processing at the moment.

In the second instance, if Chinese organizations may monitor individuals’ behaviour which is taking place in the EU, they will fall under the territorial scope of GDPR (Article 3[2][b]). Recital 24 states that to define what is monitoring the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the

\(^{31}\) Following the logic of the recent ECJ preliminary decision on joint controllership in June 2018 interpreting controllership broadly in order to ensure effective and comprehensive protection of data subjects. See Case C-210/16 Wirtschaftsakademie Schleswig-Holstein, at para. 45.

\(^{32}\) The app use is a difficult case here. Though EDPB’s emphasis on the exclusive targeting at EU market is rather clear, in practice the seemingly clear line can easily be blurred. For instance, a Chinese Dutch citizen can download a Chinese version of WeChat in China, which is a most used Chinese social networking app with multiple functionalities, and continue to use it when she returns to EU. In this case, the threshold guideline on targeting provided by EDPB’s consultation paper (especially example 9) is not a good fit of the reality.

\(^{33}\) In this case, the role of App stores including for example Apple Store and Google Store needs to be discussed since they play quite different roles in filtering and monitoring the operations of such Apps in their codes of conduct and law compliance. Controller can be defined as the main investor and owner of the app who invests money and human resources as well as material resources into getting an app built for its sole purpose and ownership rights. See Judi Oledo, Why every EU mobile app development company need to implement GDPR?, https://www.selfgrowth.com/articles/why-every-eu-mobile-app-development-company-need-to-implement-gdpr (last visited Feb 27, 2019).

\(^{34}\) Though in this case they shall be defined as data processors due to their provision of cloud services and not being the one determining the processing purposes, one may challenge this position by pointing out that in many cases it is such service providers that determine what a cloud user, at least partially, may use such services for. Also, the UK Information Commissioner’s Office (ICO) issued guidance on the use of cloud computing that expressed that at least in community cloud context, a data controller can also act as a processor in case of its maintaining the cloud infrastructure, and that in public cloud context, a cloud provider can be a data controller. See Dechert LLP, The UK Information Commissioner’s Office Guidance on the Use of Cloud Computing, 3, 7-8, at https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf.

\(^{35}\) This is the classical view that adopted by most EU scholars and taught in EU law schools, although this is really debatable because the GDPR never defines what cross-border transfer is.
internet including potential subsequent use of personal data processing techniques which consist of profiling a
natural person, in particular in order to take decision concerning him or her or for analysing or predicting his or
her personal preferences, behaviours, and attitudes. The EDPB also considers behavioural monitoring by means
of tracking through other types of network of technology involving personal data processing, e.g., by wearable
and other smart devices. Also, the EDPB pointed out the significance of intention and purpose in such monitoring
activities, and lists a number of such activities including behavioral advertisement, geo-localisation activities,
online tracking through using cookies or other tracking techniques, personalized diet and health analytics
services online, CCTV, market surveys, and other behavioural studies, and monitoring or regular reporting of an
individual’s health status (Petrovici, 2018, p. 18).

A typical example would be that when an EU resident regularly visits a Chinese website (in Chinese or an
EU MS language but host on a Chinese server), his or her personal data are collected and processed via multiple
means, including cookies (of various nature and with different functionalities and owners) or canvas
fingerprinting, to name two among others (Kirk, 2014). Or even further, he or she may registry on an online
forum and post comments and communicate with other visitors, either in Chinese or not. This person thus can be
identifiable or identified, and his or her data can be profiled, even via automated means. The monitoring can be
conducted for different purposes including providing better services or simply for the functionality or security of
the website at stake. And thus apparently, there is the overlap between providing services and monitoring in
processing practices in that in many occasions providing service needs to monitor the users to different extents
even without payment, and in many occasions, the service is free because users allow their service providers to
collect and process their data in exchange for such services provided in China.36 In this context, operators of most
Chinese smart phone apps (and apps on other portable devices and desktops) in China which are used in EU will
fall under Article 3 due to their monitoring activities in addition to providing services for a fee or not.

As discussed above, a considerable number of entities and organizations based in China will fall under
Article 3 of the GDPR. If they do not follow GDPR’s obligations and meet the requirements relating to their
processing operations as (joint)-controllers or processors, they may encounter the risk of law breaching and
subsequent administrative penalties (in theory), as well as potential litigations initiated by harmed EU data
subjects. Though EU data protection supervisory authorities would not directly impose administrative fines on
them, simply because they will not risk demeaning their authority when non-compliance on Chinese territory is a
matter of fact, they can still request them to stop or suspend processing, or cooperate for further investigation, or
may simply block access to their services in MS concerned. In this context, it is still a significant issue of rising
concern for both the EU and Chinese sides. What data controllers and processors in China shall do is an important
issue, if they intend to continue carrying out business on EU market legally.

In this context, most Chinese digital giants have already made substantial preparations long before the
enforcement of GDPR on May 25, 2018. Alibaba already established one data centre in Frankfurt, and announced
to establish a second one in EU for data localization.37 Xiaomi announced its new privacy policy that complies

36 For a bit bite of the going for free story, see Cyrus Lee, Report: Chinese users will drop WeChat if no longer free ZDNet,
https://www.zdnet.com/article/report-chinese-users-will-drop-wechat-if-no-longer-free/ (last visited Jun 18, 2018).
37 See https://www.alibabacloud.com/help/doc-detail/40654.htm &
http://www.datacenterdynamics.com/content-tracks/colo-cloud/alibaba-plans-second-european-data-center-potentially-in-the-uk-or-sweden/99040.fullarticle.
with the GDPR data transfers and processing requirements.\textsuperscript{38} The international version of Wechat, which is a Chinese version of Facebook but much more powerful with multiple functionalities, including online payment and very popular among Chinese Europeans and overseas students, updated its privacy policy in early May for law compliance (Murgia, 2017; Kharpal, 2017).\textsuperscript{39} Huawei declared that its cloud service business adheres to the Cloud security certification-CSA-STAR.\textsuperscript{40} As a matter of fact, any Chinese controllers and processors with setups or establishments in the EU as discussed above must comply with GDPR because they are directly under the jurisdiction of data protection supervisory authorities in MS and EU courts. They shall comply with the GDPR and other data protection laws strictly to the same level of EU controllers and processors even with very high costs.\textsuperscript{41} The most difficult and thus challenging issue for Chinese multinational organizations is how to ensure the level of protection when they further transfer EU resident’s personal data back to China for processing, or to a third country for processing via China (or even further directly to a third country). Because China is not listed by the Commission as providing adequate protection, they need to take further substantial steps for lawful cross-border transfers to ensure appropriate protection, such as by following approved codes of conduct (CoCs) or standard data protection clauses.

However, data controllers and processors in China without any “physical establishment” in EU now are facing a rather complex situation and need to make their decision on: Whether or not they shall comply with GDPR (as a foreign law), and if so, to what extent? If they are willing to comply with GDPR, then full compliance cost can be rather high, considering the various GDPR obligations including the technical and organizational measures to guarantee and realize the listed processing principles (Art. 5-11), different obligations of controllers and processors (including designating data protection officers and representative in EU), requirements for lawful cross-border data transfers, assisting the exercise of data subject’s rights, etc. They may need to reform their data processing operation practices or even the whole business model for full compliance. SMEs may have fewer obligations than big companies and institutions, although they do not need to keep records or appoint data protection officers (compulsory with staff number over 250).

However, an important consideration for non-compliance or simple ignorance of the GDPR rules is that regarding data breach or GDPR violation, it can be the case that EU data subjects have difficulty firstly in finding what GDPR violation may happen in China, and secondly in initiating a complaint to EU data supervisory authorities, considering the fact that China will not genrally accept the jurisdiction of EU data protection authorities and EU courts (Zhao & Bonnici, 2016; Zhang, 2013). Till February 2018, China has signed about 10 mutual legal assistance treaties with EU MSs concerning recognition and enforcement of court judgments (Wu, 2018),\textsuperscript{42} but there is almost no case reported on the Chinese side. The general reluctance of Chinese court to

\begin{itemize}
  \item See https://www.mi.com/us/about/new-privacy/.
  \item See https://www.wechat.com/en/privacy_policy.html. One has to note that Wechat has its establishment in Milan already for a while and now has been expanding its services in Europe.
  \item See http://mobile.163.com/17/0328/21/CGL5JS1L00118017.html.
  \item According to the findings of International Association of Privacy Professional and EY, Fortune’s Global 500 companies will spend totally $7.8 billion in order to ensure that they are compliant with GDPR, which means $16 million for each company. See https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/.
  \item These countries include Belgium, Italy, and Bulgaria (in civil matters); France, Spain, and Hungary (in civil and commercial issues); Poland, Romania, Greece, Lithuania (in civil and Criminal matters), Cyprus (civil, commercial and criminal issues), and Malta (in criminal issues). See Wu (2018); Malta and China ratify Treaty on judicial assistance, MaltaToday.com.mt, http://www.maltatoday.com.mt/news/national/14438/malta-and-china-ratify-judicial-assistance-treaty (last visited Feb. 28, 2019).
\end{itemize}
recognize and implement foreign court decisions may remain in the Chinese judicial system for a long while.\(^{43}\) However, this might be changed in the near future in light of some positive signs in China’s political economic developments, especially the so-called “One Belt, One Road” Initiative (Corre, 2017).\(^{44}\) It is rather clear that if China wants to be more involved in and engage with the EU market, it must more act in a way following international law standards and respect EU law. Against this backdrop, two Chinese local courts in Wuhan and Nanjing started to take the initiative to recognize and enforce foreign court judgments although on different grounds (China Law Insight, 2017). Second, the Supreme People’s Court of China recently issued an Opinions on Improvement of Judicial Assistance with the Countries Related to One Belt One Road in 2015, implying that Chinese courts may expand the scope of judicial assistance under the principle of reciprocity, even though there is no international treaty between China and the countries of concern.\(^{45}\) It might be the case that with China’s further in-depth participation in global economic order, especially in the EU market, China has to consider recognizing and implementing EU court decisions based on the reciprocity principle, because China also needs to protect her own economic interests in EU simply for fair exchange.\(^{46}\)

Further, there are also equally important considerations for controllers and processors that are in China but have no establishment in EU to comply with GDPR. On the whole, it is vital for Chinese entities (in particular companies) to gain trust and good reputation among EU customers by complying with EU laws and industrial standards, including the GDPR that levels up data protection with other fundamental rights in EU as discussed above. Needless to say, to demonstrate the required level of compliance with the GDPR will certainly promote future business image. Also, complying with GDPR’s high data protection standards, by taking the various measures and steps listed under the GDPR (including BCR, COCs, standard contractual clauses, designation of data protection officers, notification of data breach, etc.) will in reality improve data security and data protection in their own processing practices, thus gaining higher trust from Chinese clients on Chinese market. To follow GDPR data protection standards can in a way distinguish themselves from other Chinese market players.

Practically speaking, GDPR compliance, especially for SMEs in China, can be achieved to different extents by considering their own specific situations. A controller or processor in China shall make appropriate efforts to best comply with the GDPR requirements for data protection. For instance, when detecting its website visitors are from EU, the controller shall at least provide the choice of consent for collecting and processing visitor’s personal data via popping-up cookies, explaining its privacy policy and how it will use the collected data, so that it may demonstrate, at least and on the face of it, it is trying to comply with the GDPR.\(^{47}\) Thus, at least the GDPR listed procedural and organizational measures that are less costly and easier to take, shall be arranged in the first

\(^{43}\) Very few such cases can be found from China’s court database up until last year. According to an uncompleted research, only three foreign judgments are recognized or enforced by Chinese courts on the ground of the international treaties concluded by China and foreign countries. This include Foshan-Milan Case, Guangzhou-Potters Case, and Ningbo-Wroclaw Case. For a discussion, refer to http://www.guojifayanjiu.org/Admin/UploadFile/Issue/iqx13jlz.pdf.

\(^{44}\) The initiative is rather successful in Eastern and Central Europe but not without criticisms from other EU MSs when EU has no united policy to the Chinese initiative.

\(^{45}\) See http://www.court.gov.cn/zixun-xiangqing-14900.html.

\(^{46}\) But this does not mean that controllers and processors in China may escape sanctions or punishment from EU data protection authorities and EU courts in case of data breaches. There are still multiple alternative measures to affect their business, such as blocking their business websites in EU or rejecting the related person’s entry into EU border.

\(^{47}\) It is to the author’s notice that many Chinese websites including those only in Chinese have created new privacy policy for using Cookies since May 25 2018.
instance, indicating its good intention. Other potential law compliance efforts that are less expensive and possible, include appointing a data protection officer from within the institution, or by contracting a professional law compliance/privacy expert. This may also include keeping records of data processing by following the GDPR’s detailed requirements, if applicable.

Besides organizational measures, some technical measures can also be considered to improve data safety and privacy protection to different extents, such as adopting concrete measures for achieving data protection by design and by default (Article 25), including data pseudonymization, data minimization, and encryption.48 Also, they may consider applying for data protection certification or data protection seal (mark), or adopting codes of conducts (CoCs) and standard data protection clauses approved by EU authorities to both streamline their processing in approved manners and to demonstrate law compliance, if possible.49

But to which extent such GDPR compliance measures and activities can be taken will largely depends on the good will of and especially finacial capacity of controllers and processors in China, with their many GDPR duties in mind. One has to eventually recognize the hush reality that many of the GDPR obligations and requirements can hardly be enforced on them first because of their non-physical presence in EU and secon because of the short of mutual judicial assistance between EU and China. A telling example would be the GDPR duty on the processors and controllers in China to designate local represenatives in EU under Article 27. The new EDPB’s guidelines on Article 3 has affirmed the obligation of online services providers that provide services to EU residents but have no establishment in EU (Petrovici, 2018, p. 22). However, it is very dubious how many of such online services providers in China would (and are capable to) designate a representative in order to follow Article 27, even if EDPB affirms clearly that the presence of the representative within the Union does not constitute an establishment by virtue of Article 3(1) (Petrovici, 2018, p. 4). This requirement will expose most of these online business services providers in China to the risk of breaching the GDPR duty, for instance, taking into account the numerous Chinese sellers on Alibaba’s and Jingdong’s platforms and others maintaining their online selling website targeting EU consumers. In this case, the non-compliance is simply a daily reality, unless the EU data protection authorities will hunt down them one by one.

**Conclusion**

The right to data protection as a fundamental right in EU law proves to be an important legal development due to the growing significance of datafication, digitalization, and connectedness of human community. Personal data has become more and more valuable both to individuals and to society as a whole, which risks the evaporation of the control of personal life by losing control of own data. As a fundamental right, the right encounters rising challenges from the advances of new technologies and the fragmentation of jurisdictions and state laws that have been developed on the basis of national sovereignty with geographical boundaries, in contrast to our globalized, borderless morden online life.

---

48 Under Article 4(5) of GDPR, pseudonymization means 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 that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

49 One has to notice that even within the EU how such certification mechanisms shall be realized for the stated purposes is very problematic in terms of criteria establishment and further compliance monitoring.
In this context, GDPR’s strict personal data protection mechanism does not come without major problems with respect to the underlying rationale and applicability in globalized data processing practice (Koops, 2014). This is clearly evidential in the above analysis of GDPR’s potential impacts on controllers and processors in China that process data of EU residents’ and their potential non-compliance. In order to protect this fundamental right in the context of cross-border data transfers and processing, there is still much to be done in view of the hush realities of insufficient protection of the right to data protection in China. At this moment, protection of this right is largely at the mercy of controllers and processors in China in case they provide services to EU residents or monitor their behaviours in EU, but without physical presence in EU. It is also very difficult for EU residents to find their personal data being abused or misused in a foreign country; even law breaches or right violations are found, legal remeides may not be available because Chinese courts do not generally recognize EU court decisions, unless a limited number of mutual judicial assistance treaties will really work.

The enforcement of GDPR and the protection of the fundamental right in China still need more effective efforts to bridge the big gap, including more mutual judicial assistance agreements between MSs and China, together with their strict application, when an adequacy decision from EU or any agreement similar to the EU-US Privacy Shield Framework is still not feasible in the near future for China. In addition, technically speaking, data localization can be a possible, temporary solution. But this may only solve part of the problem, due to the open and borderless nature of the Internet. Unless there will be a full balkanization of the Internet (Scott, 2018), cross-border transfers and processings are, and still will be, the unescapable daily reality in the growing EU-China relationships, and the insufficient protection of EU data subject’s rights in China will remain a critical issue of rising concern.

References
Benn, S. I. (2017). Privacy, freedom, and respect for persons. In R. L. Ciochon (Ed.), Privacy and personality (pp. 3-4). New York: Atherton Press.
Berman, P. (2018). Legal jurisdiction and the deterritorialization of data. GW Law Faculty Publications & Other Works, 31. Retrieved from https://scholarship.law.gwu.edu/faculty_publications/1331
Bonnici, J. P. (2014). Exploring the non-absolute nature of the right to data protection. International Review of Law, Computers & Technology, 28, 131-143.
Brkan, M. (2016). The unstoppable expansion of the EU fundamental right to data protection: Little shop of horrors? Maastricht Journal of European and Comparative Law, 23, 812-841.
China Law Insight. (2017). Recognition and enforcement of foreign judgments in China: Progress and challenges go hand-in-hand. Retrieved December 11, 2017, from https://www.chinalawinsight.com/2017/10/articles/dispute-resolution/recognition-and-enforcement-of-foreign-judgments-in-china-progress-and-challenges-go-hand-in-hand/
Corre, P. (2017). Europe’s mixed views on China’s One Belt, One Road Initiative. Brookings. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2017/05/23/europes-mixed-views-on-chinas-one-belt-one-road-initiative/
European Data Protection Supervisor. (2015). Towards a new digital ethics: Data, dignity and technology. Retrieved June 13, 2018, from https://edps.europa.eu/data-protection/our-work/publications/opinions/towards-new-digital-ethics-data-dignity-and_en
Evans, H., & Mercer, S. T. (2018). Privacy shield on shaky ground: What’s up with EU-U.S. data privacy regulations. Lawfare. Retrieved February 5, 2019, from https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations
Flint, D. (2017a). Sharing the risk: Processors and the GDPR. Business Law Review, 38, 171-172.
Flint, D. (2017b). Storms ahead for cloud service providers. Business Law Review, 38, 125-126.
DATA PROTECTION AS A FUNDAMENTAL RIGHT

Fuster, G. G., & Gellert, R. (2012). The fundamental right of data protection in the European Union: In search of an uncharted right. *International Review of Law, Computers & Technology, 26*, 73-82.

Gutwirth, S., Poulet, Y., de Hert, P., de Terwangne, C., & Nouwt, S. (2009). *Reinventing data protection?*. Retrieved June 13, 2018, from http://www.springer.com/gp/book/9781402094972

Hondius, F. W. (1980). Data law in Europe. *Stan. J. Int'l L, 16*, 87-89.

Kharpal, A. (2017). Tencent launches WeChat Pay in Europe to challenge Alibaba’s Alipay. Retrieved September 7, 2017, from https://www.cnbc.com/2017/07/10/wechat-pay-europe-launch-tencent-to-challenge-alipay.html

Kirk, J. (2014). “Canvas fingerprinting” online tracking is sneaky but easy to halt. *PCWorld*. Retrieved May 26, 2015, from http://www.pcworld.com/article/2458280/canvas-fingerprinting-tracking-is-sneaky-but-easy-to-halt.html

Koops, B. J. (2014). The trouble with European data protection law. *International Data Privacy Law, 4*, 250-261.

LaForgia, M., & Dance, G. J. X. (2018). Facebook gave data access to Chinese firm flagged by U.S. intelligence. *The New York Times*. Retrieved June 12, 2018, from https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html

Leczykiewicz, D. (2013). *Horizontal application of the charter of Fundamental Rights*. Retrieved June 17, 2018, from https://papers.ssrn.com/abstract=2328175

Liao S. (2018). Why Facebook’s secret data-sharing deal with Huawei has the US concerned. *The Verge*. Retrieved June 12, 2018, from https://www.theverge.com/2018/6/8/17435764/facebook-data-sharing-huawei-cybersecurity

McDermott, Y. (2017). Conceptualising the right to data protection in an era of big data. *Big Data & Society*. Retrieved from https://doi.org/10.1177/2053951716686994

Molnar-Gabor, F. (2016). *Data protection Oxford constitutional law*. Retrieved March 1, 2019, from http://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e95

Mostert, M., Bredenoord, A. L., Slootb, B. V., & Deldena, J. J. M. (2017). From privacy to data protection in the EU: Implications for big data health research. *European Journal of Health Law, 25*, 43-55.

Murgia, M. (2017). Tencent expands WeChat’s ecommerce platform in Europe. *European Financial Times*. Retrieved June 19, 2018, from https://www.ft.com/content/983693ac-1543-11e7-b0c1-37e417ee6e76

Petrovic, A. N. D. (2018). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). *European Data Protection Board*. Retrieved March 1, 2019, from https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en

Purtova, Nadezhda. (2013). The Law of Everything. Broad Concept of Personal Data and Future of Data Protection Law. *Law, Innovation and Technology*. 10. 40-81.

Rodotá, S. (2009). Data protection as a fundamental right. *Reinventing Data Protection?*. Retrieved June 13, 2018, from https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_3

Savov, V. (2019). Huawei leads Chinese takeover of European phone market. *The Verge*. Retrieved February 25, 2019, from https://www.theverge.com/2019/2/14/18224614/huawei-chinese-phones-europe-market-share-2018

Scott, M. (2018). The Internet is broken. Can this group fix it? *Politico*. Retrieved June 18, 2018, from https://www.politico.eu/article/internet-governance-ottawa-regulation-balkanization-splinternet-global-jurisdiction-policy-net-work/

Sloot, B. V. (2017). Legal fundamentalism: Is data protection really a fundamental right? *Data Protection and Privacy: (In)visibilities and Infrastructures*. Retrieved June 17, 2018, from https://link.springer.com/chapter/10.1007/978-3-319-50796-5_1

Solove, D. (2018). Why I love the GDPR: 10 reasons teach privacy. Retrieved February 25, 2019, from https://teachprivacy.com/why-i-love-the-gdpr/

Solove, D. J. (2008). *Understanding privacy*. Harvard: Harvard University Press.

Wu, M. (2018). How Chinese court decisions be recognized and enforced in foreign countries. Retrieved February 28, 2019, from https://wemp.app/posts/d7d5770d-0b5e-467c-866b-0d3782371448

Zhang, W. L. (2013). Recognition and enforcement of foreign judgments in China: A call for special attention to both the “due service requirement” and the “principle of reciprocity”. *Chinese Journal of International Law, 12*, 143-174.

Zhao, B., & Bonnici, M. (2016). Protecting EU citizens’ personal data in China: A reality or a fantasy? *International Journal of Law and Information Technology, 24*, 128-150.