CHAPTER 1. Introduction

a. Reasoning of the project and current state of affairs

Since the cloud has started gaining popularity, one of the catch-phrases used about it by supporters and adversaries alike and which can indeed be read in a positive or negative manner, depending on one's predisposition, has been: "There is no cloud. It's just someone else's computer."[1] Cloud computing made its entry in the IT industry as a revolution which was meant to profoundly alter the way most of IT and digital data business had been done till then[2]. Indeed, despite the partial loss of control over data that comes immediately with its use, cloud computing has been massively successful and, apart from average users' data, a great variety of critical records are also being entrusted to it, generating ever-growing concerns about their integrity, privacy and security.

In the face of these trends around the cloud and its uses, privacy and security have grown into two somewhat competing forces attempting to balance opposing needs: privacy focuses on the need to use information against the need to protect personal data, while security is centered on the need to provide access to records against the need to stop unauthorized access[3]. The importance of these competing goals has led to a plethora of legal and regulatory ventures to strike a balance and, ultimately, to achieve a certain level of trust in digital records and their storage in the cloud[4]. A particular challenge to the whole effort has come to be the fact that different jurisdictions approach privacy in substantially different manners while an in-depth understanding of what a jurisdiction's laws may aim at, or under the rules of what particular jurisdiction certain data may be governed,

---

1 Tom Geller, *In privacy law, it's the U.S. vs. the world*, 59 Commun. ACM 21–23 (2016.)

2 See also Chapter 2.

3 Luciana Duranti, Trust in online records and data. Integrity in Government through Records Management: Essays in Honour of Anne Thurston.

4 D. Hofman, Duranti L. & E. How, *Trust in the Balance*. *Data Protection Laws as Tools for Privacy and Security in the Cloud*, 10 Algorithms 47 (2017.)

requires a tremendous analytical effort. Nonetheless, in order to protect privacy and enhance security, this effort is unavoidable.

Should one look for a single phrase to summarize why cloud computing does make a difference in the way we are handling digital information and why we should regulate all this information processing having cloud computing in our focus, a suitable passage could be the following: …"preserving information in the cloud may be a black box process in which we know, at least ideally, what we put in for preservation, and we know what we want to access and retrieve—essentially the same things we put in—but often we do not know what technology is used by cloud service providers to manage, store, or process our information"[5].

Even in the ideal case in which there was no intended malice by actors involved in the cloud, data record keeping and processing done via cloud computing poses a number of unanswered questions. As Duranti and Rogers have most recently categorized them[6], those challenges broadly refer to: managing trans-jurisdictional data flows, attributing liability for and resolving data breaches, and establishing the chain of custody when a cloud service provider goes dark[7]. Given these risks, one might wonder why people continue to trust the cloud so strongly and at such a growing pace. The answer, as it will be demonstrated soon[8], is that, from a technological efficiency point of view, there is no better option in the realm of the internet-driven world right now and the cloud stands out by far from all other available technologies. Of course, the greatest ally in dealing with such risks is constant technological innovation itself, which tries hard to keep pace with malicious and innocent challenges of the cloud alike and ensure the trustworthiness of records stored on it. However, approaches based solely on technical means cannot solve the problems that arise from technology and its maluses; besides, there is no technical solution to determined human misuse of technology, to say the least[9]. In fact, technological tools need support from legal, social, and business structures that set the

5 Luciana Duranti, Adam Jansen, Giovanni Michetti, Mumma Courtney, Daryll Prescott, Corinne Rogers & Thibodeau Kenneth, *Preservation as a Service for Trust*, in Security in the private cloud, 47–72 (John R. Vacca ed., 2017.)

6 *Id.*

7 This issue does not form part of this analysis which solely focuses on the public law aspects of cloud computing regulation, leaving civil or criminal law issues aside for future research.

8 See Chapter 2.

9 Luciana Duranti (note 3).

bar for minimum expectations from cloud service providers. While some users (particularly those heavily based on data storage and processing from their core operation model already) might indeed thoroughly analyze the "reputation, performance, competence, and confidence"[10] of cloud service providers to verify their trustworthiness and robustness, experience and market data show that the majority continue to be quite instinctive with the choice of whom they entrust with their data[11]. It is precisely for those cases – which probably constitute the majority anyway – where consumers rely upon a service without having sought assurances of its quality beforehand that the law must step in to provide the certainty and trust users cannot or did not bother to obtain on their own[12]. The typological diversity of records kept in cloud environments is forcing the law to modernize existing regulatory tools and improvise on new ones. Combined together, these tools aim to strike the balance described earlier: between long-standing concerns, namely access, control, security, and trust and a world where data have got considerably detached from the physical bonds that traditionally kept them within the borders of a single jurisdiction and the control of an identified and trusted custodian.

Discussing "privacy" as a legal pursuit is challenging to say the least; according to Solove, "Privacy seems to be about everything, and therefore it appears to be nothing"[13]. The very conception of privacy is widely contextual; as it has been argued, "our conceptions of privacy result from our juridified intuitions—intuitions that reflect our knowledge of, and commitment to, the basic legal values of our culture"[14].

On a broader basis, Americans' use of the term 'privacy' typically refers to "privacy as an aspect of liberty, the right to freedom from intrusions by the state"[15]. Consequently, American privacy laws tend to focus on the freedom to determine who and to what extent has access to one's

10 Luciana Duranti & Corinne Rogers, *Trust in digital records*. *An increasingly cloudy legal area*, 28 Computer Law & Security Review 522–531 (2012.)

11 Frank B. Cross, *Law and trust*, 93 The Georgetown Law Journal 1457–1545 (2005.)

12 Huaiqing Wang, Matthew K. O. Lee & Chen Wang, *Consumer privacy concerns about Internet marketing*, 41 Commun. ACM 63–70 (1998.)

13 Daniel J. Solove, *A Taxonomy of Privacy*, 154 University of Pennsylvania law review 477–560 (2006.)

14 James Q. Whitman, *The Two Western Cultures of Privacy*. *Dignity versus Liberty*, 113 The Yale Law Journal 1151–1221 (2004.)

15 For further analysis, see Chapter 3.

private life, particularly to the category of private information generally quoted as "personally identifiable information"[16]. From that perspective, gravity primarily lies with the possibility for a data subject to consent to their loss of privacy, while in laws developed under this prism the need for privacy is often juxtaposed by the need to use personally identifiable information for data subjects for countless different purposes. In contrast, the European concept of privacy views the term "as an aspect of dignity"[17]. The "juridified intuitions" on the foundations of European understandings of privacy cannot bear human dignity as a commodity. As a result, the American concept of 'privacy' coincides much better with the European notion of 'data protection'[18]. Both these policy areas on the two sides of the Atlantic seek to draw boundaries around information and records, putting up effective protection mechanisms for them from public or unauthorized private scrutiny. Such laws set off from the predicament that not all people can be trusted with all information[19]. In the pre-internet, offline era, this was operatively translated in controlling access to and, if necessary, retracting paper records containing sensitive information. However, under the profound impact of information and communications technologies on data and record keeping, along with an intensifying blur between "data" and "records," personally identifiable information can today be regarded as just a small subset of data[20], about which it cannot be said with certainty whether it is the original record or just an archived copy. However, this is a precarious approach as it strips the data off its context; an immediate effect is, for example, that we are no longer able to determine whether the data is 'private' for a particular purpose. Instead, by moving the protection focus at record, rather than data level, we could achieve better results. What is more, data mining and other big data techniques are increasingly rendering data-level privacy protection ineffective[21].

16 Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 New York University Law Review 1814–1894 (2011.)

17 James Q. Whitman (note 14).

18 *Id.*

19 Luciana Duranti (note 3).

20 Paul M. Schwartz & Daniel J. Solove (note 16).

21 Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Chris Hanson, James Hendler, Lalana Kagal, Deborah L. McGuinness, Gerald Jay Sussman & K. Krasnow

Based on these two poles, i.e. the European versus the American legal thinking about data protection and privacy, this study aims to take the decisive step and look into the matter from the broader perspective of technologies facilitating data processing and archiving of all kinds instead of the acts of processing and archiving per se. Those technologies are beyond doubt those collectively termed as 'cloud computing'. And because of the fact that legal research which aims to build up on an existing regime and provide better answers to tangible problems, which have nevertheless been around for a long time (with several laws that have already tried to tackle them thus making any new approach conditional to cohesion and not just innovative spirit), cannot set off from nowhere but needs to have one firm foot on actual acquis before it can take the leap forward, the starting point of endeavors of this study will largely, though not exhaustively, be privacy and data protection laws from Europe and the US.

i. The European state of affairs

The latest development out of deployment of cloud computing technologies, i.e. big data decision-making algorithms, are by nature meant to discriminate, to make distinctions based on voluminous data of a wide variety. An immediate challenge of algorithmic discrimination is the loss of judgment[22]. "The machine is incapable of determining whether a distinction is ethical or not. Unless we come up with a comprehensive theory of discrimination that can be represented algorithmically, we have no rigorous way of distinguishing between ethical and non-ethical machine-based discrimination [... however,] some of our ethical and moral criteria are so fragile, nuanced, and culturally dependent that it is not clear that the machine will ever be capable of appropriately weighing them"[23]. Still the data-driven approach to regulation of personally identifiable information runs on the assumption that by redacting or pseudonymizing the most sensitive kinds or parts of data set, we can prevent the algorithm from filling in missing information using the vast amounts of other data, quite possibly

---

Waterman, Transparent Accountable Data Mining: New Strategies for Privacy Protection (2006.)

22 Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. on Telecomm. & High Tech. L. 351–368 (2013.)

23 *Id.*

even from the same data subject, that has at its disposal. However, sealing certain bits of data which have been labeled as personally identifiable information while leaving all other data available and open to whatever techniques resourceful data holders can devise, is a lost battle. The current data-centric approach to privacy will be less and less effective in building up or maintaining trust in cloud-based records[24].

The brand new European General Data Protection Regulation (GDPR)[25] explicitly recognizes these challenges, and seeks to establish a higher standard of trust and security for EU citizens[26]. And while it does not categorically solve all big data challenges to privacy, it does provide a much firmer ground for European citizens to expect that their privacy will not be breached by resourceful data processors. Furthermore, the European Union provides a second line of legal protection for its citizens, as the GDPR directly cites Article 8(1) of the Charter of Fundamental Rights of the European Union (CFREU)[27] which has already been repeatedly interpreted as providing robust protection for the online version of the right to privacy[28]. However, the GDPR largely remains a technology agnostic

24 Jiahong Chen, *How the best-laid plans go awry. The (unsolved) issues of applicable law in the General Data Protection Regulation*, 6 International Data Privacy Law 310–323 (2017.)

25 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (OJ) L119, 4/5/2016, p. 1–88.

26 Recital 26 of the GDPR explicitly notes that, even though personal data may have undergone pseudonymization, "account should be taken of all of the means reasonably likely to be used […] to identify the natural person directly or indirectly," distinguishing between pseudonymized data and anonymous data.

27 Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

28 Recital 73 of the GDPR reads: "Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regula-

legislation[29], one that follows on the long path of data-focused EU privacy legislation, which is developed having specific existing or foreseeable applications of data-related technologies in sight instead of the specifications, present and foreseeable ones, of those technologies.

ii. The US state of affairs

The regulatory plateau in the US regarding phenomena occurring in the cloud, most prominently regarding the issue of how to gain access to data hosted on cloud environments, is substantially different to the one in Europe; not so much as to the aims it pursues or the genre of protection it wishes to grant to data subjects but rather on the way it has developed over the years and how it looks today[30]. Owing to the endemic differences of legal tools between Europe and America, in the US there is no central legislation regarding cloud data but rather several legal resources (from provisions of the US constitution, to Acts, to case law) which provide legal basis for regulating cloud-related phenomena. The global clouds on which the greatest part of the IT world operates today pose challenging questions regarding the scope of traditional legal tools governing these phenomena and, most importantly, the issue of access to data stored in cloud facilities outside the United States. The far from settled landscape on the issue can be observed even through latest case law with regard to the Stored Communications Act (SCA)[31]. Different decisions expose numerous unan-

---

ted professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behavior under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.".

29 For more extensive analysis on the GDPR and its shortcomings as well as the innovations it introduces refer to Chapter 4.

30 For a comparative analysis on the development of data protection and privacy law in Europe and the US refer to Chapter 3.

31 The Stored Communications Act (SCA), 18 U.S.C. Chapter 121 §§ 2701–2712. For more refer to Chapter 3.

swered questions about the conditions under which parties can obtain cloud data. Specifically, in litigation involving extra-territorial data requests under the SCA US courts have at times focused on where the requested data is located, and on other instances on where the search or seizure of it will take place[32]. In addition to the SCA, there are further statutory authorities that grant government and private parties the permission to make extra-territorial data requests, creating additional unresolved issues as well. What is more, American academia is also far from settled about the meaning of territoriality for data access[33]. This scattered playing field produces equally varying legal outcomes which themselves demonstrate how disconcerted existing US laws applying to the cloud are, their most alarming effect being that they powerfully incentivize international data localization[34]. Mandatory data localization is already a legal requirement in a number of countries such as Brazil and Russia, while there is additionally another important trend of voluntary data localization[35]. Both of them are, to a significant degree, fueled by concerns about US rules for data access, which make more and more non-US companies to choose to bind themselves to national or regional protections which recognize or demand data localization for cloud networks. However, in the long run, this trend risks seriously disrupting the Internet and undermining one of its fundamental characteristics, the lack of boundaries in the circulation of da-

32 For an overview of the latest trends and developments in US law and jurisprudence regarding data and access to them, especially in relation to the cloud and information hosted on facilities abroad, refer to: Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 Yale Law Journal 326–398 (2015); Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stanford Law Review 729–789 (2016); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 Stanford Law Review 285–329 (2014); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 University of Pennsylvania law review 373–419 (2014); David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*. *iCourts Working Paper Series, No. 33, 2015* International Journal of Constitutional Law (2015); Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313–388 (2013.)

33 Paul M. Schwartz, Legal Access to Cloud Information. Data Shards, Data Localization, and Data Trusts.

34 For a thorough analysis on the issue of mandatory and voluntary data localization, refer to: Anupam Chander & Uyen P. Le, *Breaking the Web*. *Data Localization vs. the Global Internet* Emory Law Journal, Forthcoming 53 (2014.)

35 *Id.*

ta and overall traffic[36]. Therefore, it is high time for the US to work with other jurisdictions, primarily with the EU, towards developing internationally harmonized rules for access to cloud information.

iii. Current state of affairs in other countries

In response to growing concerns about security and privacy of data in the cloud, regulators in jurisdictions around the world are turning to data localization measures[37]. These regulatory tools include laws, regulations, and policies designed to make sure that data and records are accessed, processed, and stored within a specific jurisdiction[38]. Data localization measures are conceptualized with the aim of fortifying the privacy rights of data owners whose records cross jurisdictional borders[39].

Briefly, data localization laws are based on the assumption that, if the jurisdictions in which records and data can be accessed, processed, and stored are limited, those records will be sealed against bad actors for whom laws from other jurisdictions would provide no effective recourse. Realistically speaking though, this is a problematic assumption[40]. Any records and data made available at some point online can eventually be accessed and harmed by malicious actors in almost any jurisdiction. And, of course, whether or not the jurisdiction in which the records are located can provide effect remedy in such an instance depends on more than just localization laws. Secondly, data localization laws assume that records hosted locally are by default more secure[41]. However, there is no guarantee for that; everything depends on adequate technical solutions and expertise being available within the jurisdiction where cloud services are provided. To put it plainly, it should not be taken for granted that there are actual data centers and hardware facilities by all cloud providers within the area of every single jurisdiction. In addition, data localization laws assume that local custody is a preferable means of protecting records and data and as-

36 Paul M. Schwartz (note 33).
37 Anupam Chander & Uyen P. Le (note 34).
38 *Id.*
39 *Id.*
40 Paul M. Schwartz (note 33).
41 Y. Tian, *Current Issues of Cross-Border Personal Data Protection in the Context of Cloud Computing and Trans-Pacific Partnership Agreement. Join or Withdraw*, 34 Wisconsin International Law Journal 367–408 (2016.)

suring their trustworthiness. However, this predicament invalidates the very important element of evaluation of trustworthiness that any cloud service provider, regardless of their size, should undergo in order to survive on the market according to internationally accepted market practice[42]. The last assumption is that data localization laws provide augmented stability should cloud services prove untrustworthy or insecure, because, at least, they provide clarity as to which jurisdiction's laws will apply in resolving the disputes that may arise. In reality, however, there is no better safeguard for security of records and data in the cloud than the trust mechanisms of the international cloud market, only by taking part in which can a cloud service provider, regardless of size, survive and remain competitive; thus, all CSPs will do whatever it takes to make sure they remain part of it[43].

b. Research question and structure of the project

Given the state of affairs described above, this project is going to look for ways for achieving better coordinated regulation of the cloud and the issues arising from using it. The stated aim will not be pursued though having in mind the establishment of an international regulatory framework for the cloud, let alone the introduction of some other type of supranational jurisdiction for cloud and IT-related phenomena. Instead, in an attempt to be realistic in the way the research question is approached in conjunction with the regulatory state-of-the-art across jurisdictions, the project's focus will be on pinpointing and bringing together best practices regardless of their origin which, if combined and taken into consideration as the foundations for the future development of cloud regulation laws by law makers from all legal orders will lead to a more coherent governance scheme for cloud computing. Logically, some of the suggestions put forward in the course of this analysis may not sound as ground-breaking for all readers, depending on whether each one of them is more familiar with the European or US legal thinking on the matter. However, the originality of this analysis lies precisely on drawing for the first time the best each and every school of thought has to offer under the same roof.

---

42 Nicholas Platten, *Protectors of Privacy: Regulating Data in the Global Economy – By A.L. Newman*, 48 JCMS: Journal of Common Market Studies 453–454 (2010.)

43 *Id.*

The forthcoming analysis should be read in light of the following understandings:

– Although from a technical point of view it is always easier to discern between cloud computing per se and specific applications made possible thanks to the cloud, this distinction has not yet been unquestioningly achieved on the regulatory front. Therefore, while the technical parts of this research invariably refer to cloud computing generically, in the parts of legal analysis it is mandatory to begin discourse from the laws currently applicable in order to understand how the current status has been consolidated and how steps forward could be taken. Therefore, in parts of this project where the legal dimension of the research question is dealt with the starting point is mostly, but not exclusively, existing laws about privacy, data protection and data transfers on the cloud. It is hoped that by applying the findings and suggestions presented throughout this study, current laws will move forward towards a more generic and less case-based direction, grasping the cloud phenomenon per se and not limiting their understanding to specific cloud applications.
– With regard to the jurisdictions and the origins of scholarly opinion that form part of this comparative analysis, it needs to be pointed out right from the beginning that there is a similar distinction between resources and literature of a technical and those of a legal nature. in particular, given that, from a technological perspective, the cloud is viewed in the same manner worldwide, this study utilizes relevant resources from a variety of origins (e.g. from European, American, Chinese and Canadian academics, to name a few). However, due to the greatly varied ways in which the cloud has been viewed so far from a legal point of view, only the laws and regulations of the EU and the US form part of this study. The two jurisdictions together account for the biggest part of the ways in which law makers currently deal with the cloud[44]. Moreover, this choice was also made due to practical factors, namely ease of access to resources, linguistic capabilities of the researcher (these two are the main reasons why the Chinese jurisdiction is left out of the scope of the project altogether) as well as time constraints for the completion of the project.

44 For more on the significance EU and US laws and markets play with regard to cloud computing refer to Chapter 3.

With the above understandings in mind, the chapters of the analysis that follow deal with these groups of challenges[45] regarding the prospect of a more consolidated regime on cloud computing regulation:

– The jurisdictional challenge, mainly dealt with in Chapter 6;
– The privacy and security challenge, mainly dealt with in Chapter 7;
– The convergence challenge, mainly dealt with in Chapters 8, 9 and 10.

45 Y. Tian (note 41).