CHAPTER 6. Jurisdiction and accountability in the cloud

a. Introduction – scope of this chapter

Having defined the research methodologies that will be utilized in the context of this analysis, the following chapters will be dedicated in presenting findings and putting forward proposals with regard to regulation of legal issues arising from on involving cloud computing as the standard technology for facilitating the vast majority of uses and processes it today's IT landscape. For starters, one needs to examine the main issues that any regulatory scheme applying to the cloud should deal with. Therefore, in the following two chapters we will consider the questions that any kind of legislative text meant specifically for cloud computing and its applications should provide answers for before, ultimately, moving on to bringing together proposals and best practices from either the EU or the US school of thought regarding the cloud and arguing on how these could be better coordinated between the two jurisdictions. At first, in the present chapter the issues of who is accountable for incidents occurring in a cloud-based environment and how authorities or courts claim jurisdiction to adjudicate on these incidents will be examined.

PART I: Jurisdiction in the era of cloud computing

a. The currently prevailing legal norms in EU law for claiming jurisdiction over cases involving data transfer and processing

Given the lack of a body of legislation specifically dealing with cloud computing, one needs to look into neighboring fields of legislation in order to describe the current status quo about how laws dealing with issues involving digital data claim jurisdiction among each other.

As it has been explained already[469], EU laws are the ones with the most articulated reasoning in matters related to the Internet and its implement-

469 See Chapter 3.

ing technologies[470]. The most representative piece of law among all IT-related EU legislation is the General Data Protection Regulation. Since we currently are at the crossroads between the GDPR and its long-lived predecessor, the Data Protection Directive (DPD), it is worth analyzing how both these laws settled the issue of territorial and material scope for their provisions. In this way, it will be possible to draw conclusions with regard to the trend EU laws follow on this matter, which, it can already be briefly stated that it is expansive.

Firstly, then, in the DPD three main grounds were described as the ones that suffice to justify jurisdiction on an IT-related case. In particular, the GDPR's forerunner generally recognized three different grounds for determining its applicability on personal data processing affairs. These were:
– establishment of the data processor under examination[471],
– public international law[472] and
– use of equipment within the jurisdiction[473].

In a cloud computing context, the above grounds determined the extent to which a user or provider of cloud computing services, even if not incorporated, residing or headquartered in an EEA Member State, could become subject to obligations under EU data protection law as a result of:
– having a subsidiary, branch or agent, or a mere data centre, in the EEA; or
– making use of a data centre located in the EEA, or other equipment located in the EEA.

i. Establishment – Art. 4 para. 1(a) DPD

The DPD stipulated that each EEA Member State had to apply the Directive's provisions as this was implemented in that Member State if 'the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'. In other words, the controller had to have an establishment on the ground of that Member

470 See also Chapter 2.
471 Art. 4 para. 1(a) Directive 95/46/EC (DPD) (note 143.)
472 Art. 4 para. 1(b) Directive 95/46/EC (DPD) (note 143.)
473 Art. 4 para. 1(c) Directive 95/46/EC (DPD) (note 143.)

State and should process personal data 'in the context of the activities of that establishment'.

In fact, what is described above is, one could say, a two-step test as it was examined whether

– the data controller has an 'establishment' on the territory of an EU Member State, and
– whether the controller processes personal data in the context of the activities of that establishment.

If the answer to both questions was yes, then the Member State which hosts the data controller on its soil had to implement the DPD to personal data processing activities carried out by that controller, regardless of where in the world they took place – outside or inside the EEA.

It is worth briefly mentioning that the criterion of 'the context of the activities of an establishment of a controller', which was among the main ones in EU law under the Data Protection Directive had, over the years and with the evolution of technology, come to cause a great deal of friction as to its precise interpretation[474]. In the latest years when the DPD was still in force, Art. 29 Working Party had stated three factors which should be taken into account when assessing this criterion[475]:

– the degree of involvement of the establishment(s) in the activities in the context of which personal data are processed;
– the nature of the activities as a secondary consideration and
– the goal of ensuring effective data protection.

Art. 29 WP went on to suggest that a 'who is doing what' test should be applied in the sense that the test required a determination of:

– who carries out the relevant activities and
– whether there is data processing in the context of these activities.

The involvement of the establishment in the activities is the most important of these factors.

The wide interpretation of 'in the context of the activities of an establishment' that was put forward meant that a cloud provider with one or

474 Joel Reidenberg, *Technology and Internet Jurisdiction*, 153 University of Pennsylvania law review 1951–1974 (2005.)

475 Article 29 Working Party, Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

more establishments in the EEA was also subject to this provision. This had two important consequences[476]:

– EU data protection law could be applicable even if no processing of personal data was carried out at the establishment of the cloud provider, and
– because of the nature of cloud services and the geographical dispersion of their facilities, more than one establishment of the same cloud provider in the EEA may be involved in activities, so that the controller is subject to two different national implementations of the DPD.

One contemporary case, sparked by the use of technological resources heavily based on cloud computing technology that is demonstrative of how loosely Europe has been interpreting until now the criteria it upholds for determining jurisdiction on a cloud computing related case was the so called 'Google Italy'[477] one.

The case referred to a video which was posted on September 8, 2006 in Google Videos showing a disabled student being bullied and insulted by three of his colleagues (while another student was recording with her mobile phone, and ten more were watching the scene without intervening). The video, with a duration of about 3 minutes, was viewed by a significant number of people, counting more than 5000 downloads. Eventually it had made it to being the most popular one in the category of "video divertenti" (funny videos). Users of Google posted various messages in the comments section of the video; apparently, some flagged it as being inappropriate and some e-mailed Google requesting for it to be removed. On 7 November 2006, the Italian Postal Police, after a communication from a citizen, requested Google to remove the video, which was deleted on the same day. As a result, the video had been available in total for about two months after it was initially posted. On the aftermath of the incident, three lawsuits were filed against

– the students molesting the victim of the bullying attack on the video
– the teacher and school authorities of the facility where the incident took place for failing to prevent the incident
– Google Italia and its executives for criminal defamation and violation of data protection rules. With regard to data protection, the accusation

476 *Id.*

477 Raul Mendez, *Google case in Italy*, 1 International Data Privacy Law 137–139 (2011.)

was that Google Italy was processing personal data, and in particular health data, illicitly, for the purpose of making a profit[478].

Leaving aside all other aspects of the case, it is worth summarizing the main findings related to the issue of responsibility of the internet service provider (in this case, Google and its cloud based service Google Videos), which was found to exist by application of the very broad in scope EU legislation[479] in force at the time. A major part of commentary has found the decision of the Italian judge in this case defective in various regards. Most importantly, the decision was slammed because it failed to conceptualize the role of platform providers in the context of the web 2.0[480], and their enabling function with regard to user-driven generation of contents; in other words, it failed to understand the edgy difference of cloud empowered platforms. In any case, this was just one example of several similar cases that arose during the years of the DPD which, especially as cloud technologies were taking more and more over older conventional IT solutions, made clear that the cloud era brought with it the need for a profound shift in the ways in which jurisdiction was recognized in relevant affairs.

ii. International law – Art. 4 para. 1(b) DPD

The second criterion through which EU law in the years of the DPD determined jurisdiction in data processing and handling matters is that of international law. Precisely, European data protection laws applied where the controller was not established on a Member State's territory, but the law of at least one Member State applies by virtue of international law[481]. Such would be, for instance, the case of a ship or aircraft under a particular Member State's flag. In the context of cloud computing, this may be rele-

478 Sentenza n. 1972/2010. Tribunale Ordinario di Milano in composizione monocratica. Sezione 4 Penale. Available at http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf (16.02.2016). P. 102/103.

479 G. Sartor & Viola de Azevedo Cunha, M., *The Italian Google-Case. Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, 18 International Journal of Law and Information Technology 356–378 (2010.)

480 Tim O'Reilly & John Battelle, Web Squared: Web 2.0 Five Years On.

481 W. Kuan Hon, Julia Hörnle & Christopher Millard, *Data Protection Jurisdiction and Cloud Computing. When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3*, 26 International Review of Law, Computers & Technology (2012.)

vant for cloud facilities, e.g. data centers, which may be set up on vessels or platforms floating outside the territorial waters of any Member State[482].

iii. Equipment – Art. 4 para. 1(c) DPD

The final grounds on which the DPD had been traditionally basing jurisdiction to apply its data protection law in cases relevant to the provision or use of cloud computing services was the 'equipment' criterion[483]. Under this, even if the data controller 'is not established on Community territory', the application of a Member State's data protection law may nevertheless be valid if this controller 'makes use of equipment, automated or otherwise, situated on the territory' of that State for the purposes of processing personal data, unless the equipment is only used 'for transit through' Community territory. We should also not fail to point out that there is no requirement that the personal data processed had to relate to EEA individuals.

iv. Changes to current status quo by the upcoming GDPR

Under the newly arriving regime of the GDPR, the issue of material and territorial scope of European legislation on data processing and transfers (still the piece of law closest to the nature of the data related activities executed via cloud computing) will become even broader. In particular, the GDPR will apply to organizations which have EU "establishments", where personal data are processed "in the context of the activities" of such an establishment[484]. As long as this test is met, the GDPR applies irrespective of whether the actual data processing takes place in the EU or not. The term "establishment" was analyzed by the Court of Justice of the European Union in the 2015 Weltimmo vs. NAIH case[485]. In there the

---

482 While this may sound futuristic, Google has obtained a patent in the United States for such data centers built on ships. So in future there may well be data centers on ships moored outside territorial waters, with the possibility of flags of convenience being used for data protection law purposes.

483 W. Kuan Hon, Julia Hörnle & Christopher Millard (note 472.)

484 Art. 3 para. 1 Regulation (EU) 2016/679 (GDPR) (note 25.)

485 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14, (OJ) ECLI:EU:C:2015:639.

CJEU confirmed that establishment is a "broad" and "flexible" phrase that should not hinge on any particular legal form. An organization may be "established" where it exercises "any real and effective activity – even a minimal one" – through "stable arrangements" in the EU. The presence of a single representative may be sufficient. In that case, Weltimmo was considered to be established in Hungary as a result of the use of a website in Hungarian which advertised Hungarian properties (which meant, according to the Court's interpretation that it was "mainly or entirely directed at that Member State"), use of a local agent (who was responsible for local debt collection and acted as a representative in administrative and judicial proceedings), and use of a Hungarian postal address and bank account for business purposes – even though Weltimmo was incorporated in Slovakia. Organizations maintaining EU sales offices, which promote or sell advertising or marketing targeting EU residents, are therefore expected to be subject to the GDPR as well – since the associated processing of personal data is considered to be "inextricably linked" to and thus carried out "in the context of the activities of" those EU establishments[486].

Non-EU established legal entities will be subject to the GDPR as well whenever they process personal data about EU data subjects in connection with:

– the "offering of goods or services" (payment is not required);
– "monitoring" of their behavior within the EU[487].

For the criterion of "offering of goods and services" (but not monitoring) to be fulfilled, mere accessibility of a site from within the EU is not sufficient. It must be apparent that the organization envisages that activities will be directed to EU data subjects. Contact addresses accessible from the EU and the use of a language used in the controller's own country are also not sufficient. However, the use of an EU language or currency, the ability to place orders in that other language and references to EU users or customers will be relevant indications that will be taken into account and assessed. The CJEU has examined when an activity (such as offering goods and services) will be considered "directed to" EU Member States, even though in a different context unrelated to data processing (i.e. under the "Brussels 1" Regulation (44/2001/EC) governing jurisdiction in civil and

486 Google Spain SL, Google Inc. v AEPD, Mario Costeja González, Case C-131/12, (OJ) ECLI:EU:C:2014:317.

487 Art. 3 para. 2 Regulation (EU) 2016/679 (GDPR) (note 25.)

commercial matters[488]). Its comments are one of the few leads we have so far in our effort to interpret the same aspect of the GDPR. In addition to the considerations mentioned above, the CJEU notes that an intention to target EU customers may be illustrated by:

– "patent" evidence, such as the payment of money to a search engine to facilitate access by those within a Member State or where targeted Member States are designated by name; and
– other factors – possibly in combination with each other – including the "international nature" of the relevant activity (e.g. certain tourist activities), mentions of telephone numbers with an international code, use of a top-level domain name other than that of the state in which the trader is established (such as.de or.eu), the description of "itineraries from Member States to the place where the service is provided" and mentions of an "international clientele composed of customers domiciled in various Member States"[489].

It should be noted though that this list is not exhaustive and the question should be determined on a case-by-case basis, especially until a certain amount of time has passed by after the GDPR officially enters into force and enough experience from its actual implementation is accumulated.

It is not clear at this transitional point between the DPD and GDPR eras whether non-EU organizations offering goods and services to EU businesses (as opposed to individuals) will fall within the scope of the "offering goods and services" test in Article 3(2)(a) GDPR. "Monitoring" specifically includes the tracking of individuals online with the intention of creating profiles, including where this is used to take decisions to predict personal preferences, behaviors and attitudes[490].

Organizations subject to the GDPR's long-arm jurisdictional reach must appoint an EU-based representative. As analyzed immediately above, under the Data Protection Directive, organizations targeting EU data subjects only had to comply with EU rules if they also made use of "equipment" in the EU to process personal data. However, this led national supervisory

488 Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement
of judgments in civil and commercial matters, (OJ) L 012, 16/01/2001 P. 0001 – 0023.

489 Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller; Joined cases (C-585/08) and (C-144/09), ECLI:EU:C:2010:740.

490 For more on profiling and automated decision making, refer also to Chapter 4.

authorities, who were seeking to assert jurisdiction, to develop arguments that the placing of cookies, or requesting users to fill in forms, would amount to the use of "equipment" in the EU. It is hoped that the GDPR provisions will make easier to demonstrate that EU law applies; although, whenever organizations have no EU presence, enforcement may be just as difficult as before.

From the above, it becomes apparent that EU data protection law creates for itself an ever-wider space of material and territorial scope. The same can generally be said for any jurisdiction, in principle: every legal order is inherently striving to impose itself as much as possible over others wishing to secure for its subjects an as extended as possible (physical as well as material) vital space of legal security. This, however, respectively increases the chances for conflicts among jurisdictions. Therefore, the need for coordination among different legal orders grows even more important so that frictions and jurisdictional uncertainty are avoided, as much as possible. Shifting the focus from data processing as a particular activity to cloud enabled processes involving data in general and developing cloud computing regulation rules through this generic perspective will offer a much more suitable ground for common understanding among different legal orders.

b. Technology and internet jurisdiction: a process of parallel 'give and take'

The rise and evolution of technology, especially in the field of IT, has decisively defined many different aspects of people's lives over the latest decades. Reasonably, this technological omnipresence has also spurred new legal disputes and cases that called for adjudication. As a result, this new genre of legal cases has affected all different aspects of judicial procedure including the one of determination of jurisdiction. Initially, cases that were born out of technological evolution were mostly seeking to deny jurisdiction, choice of law, and enforcement to states where users and victims were located[491]. Those cases have been described by a certain num-

491 Joel Reidenberg (note 474).

ber of scholars as a type of "denial-of-service" attack[492] against the legal system, in particular to the jurisdictions of users and victims.

However, after this initial type of technology-spurred cases that threatened to stir an imbalance between jurisdictions of countries that were home to IT providers over those of users or victims of malicious practices involving IT innovations, the trend was reversed[493]. The continued surge in IT has already tamed and will further undermine the initial technological assault on state jurisdiction. This reverse of the tide was made possible thanks to the fact that as computing gets more sophisticated, so it enhances the processing capabilities and power of users' computers[494]. These technologically advanced machines are gradually giving to the victim's state a wider nexus of tools for dealing with offending acts, while it greatly facilitates the establishment of a direct relationship with the offender for purposes of personal jurisdiction and choice of law[495]. Even more, some of these innovations additionally enable states to enforce their decisions electronically and, consequently, bypass the problems of foreign recognition and enforcement of judgments[496].

This peculiar 'war' between exercises of state power through assertions of jurisdiction and technologically spurred legal issues has proven to be beneficial for technology itself[497]. In fact, out of this friction came considerable momentum that helped the advancement of pioneering granular technologies[498] and the consolidation of new service markets for legal compliance[499].

In conclusion, the assertion of sovereign jurisdiction to protect citizens might indeed be a tricky thing that is far from being settled and, actually, it urgently needs to be revisited. Additionally, another aspect of the matter is that the phenomenon is likely to advance the fundamental public policy premise that the rule of law should be supreme to technological determin-

---

492 Sean P. Kanuck, *Information Warefare: New Challenges for Public International Law*, 37 Harv. Int'l LJ 272–568 (1996.)
493 Joel Reidenberg (note 474).
494 Joel Reidenberg (note 173).
495 Reidenberg, J. R., Schwartz, P. M. (note 174).
496 Joel Reidenberg (note 175).
497 Joel Reidenberg (note 474).
498 *Id.*
499 Lawrence Lessig & Paul Resnick, *Zoning speech on the Internet: A legal and technical model*, 98 Michigan Law Review 395–431 (1999.)

ism[500]. Nevertheless, the multiplicity of states with jurisdiction over Internet activities is also likely to stimulate creativity towards new Internet services such as more accurate and selective filtering technologies, stronger security zones and more robust, customized compliance capabilities via sophisticated applications. In that sense, and taking for granted that the variety of choice on the jurisdictional front is not going to cease from existing any time soon, an attempt to build a minimum threshold of understanding between competing jurisdictions about what they view and understand as 'cloud computing' or by other terms related to IT advancements and applications could even serve as one extra catalyst that would accelerate innovation. 'Playing' with known rules but, at the same time, having to come up with arrangements that will work with all different interpretations of these rules is a condition favorable to technological evolution[501].

These observations are also backed by two of the most prominent academics in the field of IT law and regulation[502]. From one side, Paul Schwartz has formulated the thesis that "different parties in the cloud can contribute inputs, outputs, analytics, and execute different kinds of actions. The result of this distributed computing environment is to permit dramatic flexibility in processing decisions – on a global basis."[503]

On the other side, Lawrence Lessig has portrayed this unconventional relation between legal rules and technological capacities with an emphatic dictum: "code is the law of cyberspace."[504] Indeed, the architecture of the internet – its code, network protocols and enabling technologies – is what determines what can or cannot be done on the network[505]. Lessig went so far to actually suggest that "as the underlying code of the network ultimately dictates the rules to which users are compelled to obey (whether or not these rules are actually endorsed by the law), it becomes a de facto law"[506].

---

500 *Id.*
501 Joel Reidenberg (note 474).
502 E. Kosta, Consent in European Data Protection Law (2013); Steffen Kroschwald ed. (note 317).
503 Reidenberg, J. R., Schwartz, P. M. (note 174).
504 L. Lessig, Code and other laws of cyberspace (1999.)
505 Lawrence Lessig, *Law Regulating Code Regulating Law*, 35 Loyola University Chicago Law Journal 1–14 (2003.)
506 Joel Reidenberg (note 474).

c. From data protection law to international jurisdiction on the internet; adapting laws to modern needs and reality

As defined under public international law 'jurisdiction is a State's right to regulate conduct in matters not exclusively of domestic concern'[507]. It needs to be made clear that the notion of 'jurisdiction' must not be confused with neighboring terms as choice of law, 'conflict of laws', or 'applicable law', which deal with the question of which law or laws shall be applied in a given case. However, as the complexity of matters seeking judicial remedy increases, jurisdiction and choice of law as concepts become closely related, and the distinction between them has become increasingly vague[508].

In an effort to trace the updated meaning of 'jurisdiction' when it comes to issues stemming from cloud computing technologies, one may depart from neighboring legal fields which are already sufficiently regulated. Probably the closest field from which useful information could be extracted to serve as the basis for a theoretical discourse about the question of jurisdiction in cloud computing matters is that of data protection. Data protection law should not be regarded as falling entirely within either private or public law. In fact, the body of law known today as data protection derives from a wide variety of legal sources, namely consumer protection law, human rights law, internal market law, and others[509].

As Jon Bing has stated: 'Data protection legislation will typically contain provisions of a public law nature, relating to an authority and its duties and decisions. But the law will also often include civil law provisions, typically on liability for data protection violations. The provisions of data protection legislation may therefore have to be qualified as belonging to different areas of law, to which different relevant connection criteria are assigned. Following the traditional method, different aspects of one case may then have to be decided by different lex causae, which easily may lead to distortions as the legislation is conceived as an organic whole

507 C. Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, 18 International Journal of Law and Information Technology 227–247 (2010.)

508 *Id.*

509 C. Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1)*, 18 International Journal of Law and Information Technology 176–193 (2010.)

where the different provisions support an appropriate solution'[510]. One should not forget that the origins of data protection law in consumer protection and human rights law may also indicate that courts and data protection authorities could regard some of its rules as ordre publique, i.e. directly and unconditionally enforceable regardless of the applicable law[511].

While, as it is known, public international law only applies directly to relations between States, it also serves another purpose as the basic limiting standard of the international legal order and the testing ground for jurisdictional rules affecting private parties in different States as well[512]. In fact, even for the specific field of IT, the Article 29 Working Party has recognized that "jurisdiction under data protection law should be evaluated under public international law"[513]. Besides, the legality of jurisdictional rules under international law is important because of the global nature of the Internet. Since both major legal systems that are under focus in this study, i.e. those of the EU and the US, at least attempt to interpret domestic law in harmony with international law, the main assumptions of international law on jurisdiction can be vital in the quest for a harmonized approach on cloud related matters.

Although there is a certain degree of overlap between them, jurisdiction in international law is generally divided up into three different categories[514]:

– **Legislative or prescriptive jurisdiction**, which is 'the power of a State to apply its laws to cases involving a foreign element'[515]. Legislative jurisdiction is, at most times, concurrent rather than exclusive[516]. A very typical example of legislative jurisdiction in the area of data

510 J. Bing, *Data Protection, jurisdiction and the choice of law* Privacy Laws & Policy Reporter 92–98 (1999.)

511 Christopher Kuner, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2)*, 18 International Journal of Law and Information Technology 227–257 (2010.)

512 *Id.*

513 Article 29 Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

514 C. Kuner (note 507).

515 Uta Kohl, Jurisdiction and the Internet. A study of regulatory competence over online activity (2010.)

516 Svantesson, Dan Jerker B, Private international law and the internet (2012.)

protection law is the application of EU data protection law to a webpage located outside the EU that deploys cookies to process personal data of individuals residing within the EU area. In the field of cloud computing, one case where prescriptive jurisdiction would apply is when the servers of a cloud provider with whose resources personal data of individuals from within the EU area are processed are located outside the EU.

- **Adjudicative jurisdiction**, which means 'the power of a State's courts to try cases involving a foreign element'[517]. An example of this type of jurisdiction occurs when a European data protection authority that decides on a complaint submitted by an individual residing in the EU with regard to the processing of their personal data by an entity outside the EU. If, in addition, we consider data protection law as 'public law', adjudicative jurisdiction becomes identical to legislative jurisdiction[518]. Mutatis mutandis, an example of adjudicative jurisdiction in the realm of cloud computing occurs when a DPA investigates the practices of a cloud resources provider outside the EU, which are utilized for processing data belonging to EU law subjects.
- **Enforcement jurisdiction**, which refers to 'the power of one State to perform acts in the territory of another State'[519]. One such instance is when a European data protection authority moves to conduct an audit of an entity headquartered outside the EU. Similarly, in the case of cloud computing, enforcement jurisdiction occurs when a European DPA moves to carry out an audit on the facilities of a cloud provider headquartered outside the EU area.

It shouldn't be overlooked that the legality of any of these types of jurisdiction is closely connected with that of the other types, while any limitations on one type of jurisdiction may also have effects the scope of the others[520].

Logically, each of the different types of jurisdiction described above need a conceptual basis to be founded on[521]. The following are the juris-

517 Michael Akehurst, *Jurisdiction in International Law*, 46 Brit. Y. B. Int'l L. 145–258 (1972.)
518 Uta Kohl (note 515).
519 Michael Akehurst (note 517).
520 P. P. Craig & G. de Búrca (note 287).
521 C. Kuner (note 507).

dictional bases that have become most widely accepted, and that are most relevant to data protection law:

- **Territoriality**: Following the principle of territoriality, jurisdiction is determined based on the acts that have been committed within the territory of the judging state[522]. A variation of it is the 'objective territoriality principle', according to which the act under judgement was initiated outside but completed within the territory of the state, or a constituting element of the conduct under examination occurred within the territory of the state claiming jurisdiction[523]. Much as the territoriality principle is probably the most fundamental one for concretizing jurisdiction, the Internet greatly complicates application of it; as it has been already explained, it can be nearly impossible or resources-wise nonviable to localize an online action down to the territory of a particular State.
- **Personality:** Under the principle of personality, jurisdiction is asserted by the state of nationality of the perpetrator (active personality principle) or of the victim (passive personality principle)[524]. This jurisdictional principle is prevalent in criminal law; however, there are instances when it is applied also in civil law[525]. When it comes to cloud computing, a lot of details merit clarification before the personality principle can be applied; such as, how is the perpetrator among all those actors making a cloud-based processing possible, whether the cloud services user, who may also be the person that finally bears the burden of a cloud-based processing, can be billed as the victim of an act if he/she was also the one that had triggered off the processing etc.
- **Effects doctrine:** The 'effects doctrine' has traditionally been regarded as the most controversial of all jurisdictional bases[526]. According to it, jurisdiction is claimed based on the fact that a certain conduct outside a state has effects within the state[527]. Despite the relentless critique it has attracted, the effects doctrine seems to have become widespread, particularly with regard to assertions of jurisdiction over conduct on the

522 Svantesson, Dan Jerker B (note 516).
523 *Id.*
524 *Id.*
525 *Id.*
526 *Id.*
527 C. Kuner (note 509).

Internet[528]. The basic argument of opponents of the effects doctrine is that it is open-ended, since 'in a globalized economy, everything has an effect on everything'[529]. An additional point of friction is that 'the widening of the reach of effect based jurisdictional rules results in a widening of the gap between reasonable grounds for jurisdictional, and application of law, claims on the one hand and reasonable grounds for recognition and enforcement of foreign judgments on the other'[530].

– **Protective principle:** The protective principle has been conceptualized with the aim of protecting a state from acts committed outside its territory but which jeopardize its sovereignty[531]. Jurisdiction founded on this basis is usually limited exclusively to criminal law or serious violations that endanger the security of a country[532]; such instances would normally not include data protection violations. Besides, the focus of the protective principle is on protection of the state, not of individuals (who are the main subject of protection of data protection law)[533]. However, at least in the EU, Member States have been lately interpreting the protective principle under a much wider scope than security issues, so that it resembles an application of the objective territoriality or the effects doctrine and, of course, from that perspective many internet or cloud related issues are also included[534] (e.g. the calls for investigations on the wire-tapping of communications of civilians by foreign intelligence agencies as an anti-terrorist protective measure).

d. What is the problem with asserting jurisdiction over cloud-related cases under current EU laws?

Goldsmith and Wu, two of the most prominent figures of the wider area of IT law, have expressed the view that jurisdictional uncertainties related to

528 C. Kuner (note 507).
529 T. Schultz, *Carving up the Internet. Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, 19 European Journal of International Law 799–839 (2008.)
530 Svantesson, Dan Jerker B (note 516).
531 *Id.*
532 C. Kuner (note 509).
533 *Id.*
534 *Id.*

Internet matters have been exaggerated[535]. In fact, they try to support this estimate by putting forward the following considerations:

– unilateral assertions of jurisdiction by States on the web are no different than those they make in other areas;
– technological fixes (like geolocation) offer ways in which entities can minimize their legal exposure against overlapping and exorbitant jurisdictional claims;
– there is no need to worry about all kinds of jurisdictions, just because you are doing business online. Instead, the parties need only take into consideration the relevant laws of states that are capable of taking enforcement action in relation to their case; for instance, the states which can initiate liquidation proceedings against assets of the defendant inside their territory;
– finally, it is argued that awareness is increasing that dealing with jurisdictional issues is part of the cost of doing business on the internet. However, these 'jurisdictional threats' are not always substantial; for instance, jurisdiction under EU law against a data controller without assets in the EU but has been using cookies on its website to process the data of Europeans should be of little concern to the controller, since there is no plausible chance of enforcement.

Even if these approaches are fair, by and large, the problems caused by online jurisdictional uncertainties in the context of data protection and cloud computing appear to be more serious than these[536]. As it has been already demonstrated 'cloud computing', as a term, is not synonymous to 'data processing' but it refers to a much wider range of technologies, which serve as facilitators of many different IT applications[537]. Consequently, if we continue to resort to laws that regulate the cloud without being specifically customized for the cloud, we will continue resorting to legislation that will cover a wide variety of online data-related tasks while lacking the necessary degree of specialization, thus increasing the odds for jurisdictional conflicts.

---

535 Jack L. Goldsmith & Tim Wu, Who controls the Internet? Illusions of a borderless world (2008.)

536 Christopher Kuner, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)*, 18 International Journal of Law and Information Technology 176–202 (2010.)

537 See also Chapter 3.

Moreover, when the rules resolving jurisdictional matters with regard to a law are versed in such a broad and open to interpretation manner, while the chances that this law will indeed be enforced are not equally broad, there is an inherent risk that respect for this law from its subjects will eventually be diminished[538]. Statistics and experience prove that the gap between compliance and enforcement of European data protection law up to date has been certainly large, even within the EU[539]. At the current standpoint, which coincides with the end of the DPD era, relevant figures that can be retrieved for that piece of law speak volumes: for example[540], the Spanish DPA had stated that in 2007 it had received 8,463 notifications from data controllers about international data transfers. However, it has to be pointed out that all telephone calls, e-mails, faxes, Internet browsing activities, etc. executed between end users in Spain and countries outside the EU are also to be considered 'international data transfers' in the sense of data protection law. As a result, all these occurrences might also be subject to a duty of notification, which means that out of these 8,463 reports several can be essentially insignificant, while there may be millions or even billion others which may go on completely unreported[541].

Therefore, a balancing exercise is necessary in order for the EU body of law to acquire cloud-specific laws that will be more concrete and will primarily apply on actual instances where personal privacy and similar rights are at stake and not merely when a process fulfils the technical criteria for being defined as data processing.

e. Steps to reduce jurisdictional disputes from the perspective of EU law

Achieving greater jurisdictional clarity in conflicts related to cases caused by cloud-based applications or their uses is not possible solely by changes

538 *Id.*

539 European Parliament, Report on the First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI)) (2004.)

540 C. Kuner (note 507).

541 For the full report that served as the basis for this case study: Agencia Española de Protección de Datos, Informe sobre transferencias internacionales de datos, Julio 2007, 5 (available at: https://www.agpd.es/portalweb/jornadas/transferencias_internacionales_datos/common/pdfs/report_Inter_data_transfers_colombia_en.pdf; last accessed: 19/2/2016.)

to jurisdictional rules. It can a priori be said that, given the fragmented landscape put together by different jurisdictions, there is not one such rule, or set of rules that could both envisage all cases where jurisdiction under cloud computing law would be justified, and at the same time, avoid unjustifiably extending jurisdiction in other cases. Notwithstanding, other measures compatible with the European legal thinking and practice so far could be taken that could help jurisdictional rules become more relevant and to the point while producing a more balanced framework for protection especially in cross-border cases. Such measures could include, primarily[542]:

– greater harmonization of the law: As demonstrated already, application of a state's data protection law and assertions of jurisdiction by that state seem to go hand in hand. Consequently, greater harmonization of data protection or cloud computing laws would contribute to reducing the number and the scope of jurisdictional conflicts ignited by them. Despite the primary role EU law has played so far in personal data[543], IT and alike legislations, the respective laws around the world are inspired by divergent cultural and legal values[544]. Harmonization of data protection and similar nature laws in a comprehensive, or universal, manner is unlikely to be achieved. However, as this project maintains as its primary thesis, a lot more could be done to achieve a quasi- or even a genuinely global understanding of key notions of cloud computing technologies and their most common implementations, prime among which is, undoubtedly, data protection law (for instance, terms like 'personal data', 'data controller' or 'data processor').
– cooperation between regulatory authorities: Cooperation among national or regional regulators can greatly contribute to the concretization of the scope and impact of jurisdictional conflicts[545]. A culture of rapprochement and coordination of enforcement actions, along with the adoption of common positions on important substantive legal issues are areas of cooperation where the world's DPAs could achieve real progress in the foreseeable future.
– technical solutions: Technical means such as geolocation, which are becoming more widely available, though not a solution per se, can help

542 *Id.*
543 Refer also to Chapters 4 and 5.
544 L. A. Bygrave (note 137).
545 C. Kuner (note 509).

reduce jurisdictional conflicts by helping to 'map' the Internet, thus making it easier to limit jurisdictional uncertainty[546].

– development of a theory of reasonableness[547]: As Lowenfeld suggests, any theory developed with the aim of providing answers to the broad issue of jurisdiction, at the end of the day, attempts to strike a compromise between legal certainty and flexibility. The rules that may, at any time, be adopted "need to be clear and definite enough to lead to an acceptable degree of legal certainty, but also flexible enough to cover unforeseen and complex situations, which suggests the need for a 'safety valve' that allows jurisdiction not to be asserted even when technically it could be"[548]. This concept, code-named as the 'concept of reasonableness', is intended to help resolve particular situations, typical among which are those when there is a jurisdictional conflict between regulators in two sovereign states[549].
– The use of the reasonableness doctrine to limit jurisdictional assertions was met, primarily, with strong criticism, as it seemed too vague a criterion to be useful in practice[550]. Mann also famously argued that jurisdiction should be based on a 'link' as an objective tie to the forum that is distinct from 'mere political, economic, commercial or social interests'[551]. However, as IT evolves and its main implementing technologies become more and more defiant of conventional boundaries, such as geographical or jurisdictional borders, we need to revisit suggestions like the reasonableness test and assess how they could offer answers to modern challenges.

---

546 Jack L. Goldsmith & Tim Wu (note 535); Zachary NJ Peterson, Mark Gondree, Robert Beverly, *A position paper on data sovereignty: the importance of geolocating data in the cloud* Proceedings of the 3rd USENIX conference on Hot topics in cloud computing (2011.)

547 Andreas F. Lowenfeld, International litigation and the quest for reasonableness. Essays in private international law (1996.)

548 Dan Svantesson, *Protecting Privacy on the 'Borderless' Internet – Some Thoughts on Extraterritoriality and Transborder Data Flow*, 19 Bond Law Review 168–187 (2007.)

549 C. Kuner (note 507).

550 Svantesson, Dan Jerker B., *Privacy, the Internet and Transborder Data Flows – An Australian Perspective*, 4 Masaryk University journal of law and technology 1 (2010.)

551 F. A. Mann & Académie de droit international de La Haye., *The doctrine of international jurisdiction revisited after twenty years*, 186 Recueil des cours = Collected courses 9–116 (1984.)

– greater interdisciplinary collaboration between the jurisdiction and data protection world and the IT world: Up to this point, there has been only limited interaction between scholars, international organizations, regulators, and others working on international jurisdiction or on data protection and the members of the IT industry, who are the minds that actually make possible all the applications that have ignited the problems which are discussed in this study. However, this one-sighted approach has to change and bodies dealing with international jurisdictional issues (such as The Hague Conference on Private International Law, UNCITRAL, and others) have to turn their interest also in IT, cloud computing and data protection law[552]. At the same time, they need to invite and closely collaborate with representatives from the IT industry, who can offer the input and ideas of someone with hands-on experience on the matter.

f. The internet jurisdiction risk of cloud computing under US law

After a thorough presentation of the jurisdictional risks associated to IT law and, in particular, cloud computing given the current thinking on determining jurisdiction in Europe, it is now time to turn to the US legal system and assess how American legal thinking deals with these questions.

i. The basics about determining jurisdiction under US law

US courts have struggled over jurisdictional issues related to the internet in cases of both domestic and international nature since many years[553]. The main legal instruments through which US justice has claimed and exercised jurisdiction over this type of cases are:

– Personal jurisdiction

Generally, according to US laws, courts exert personal jurisdiction over individuals or businesses that are residents of, or that are physically located within, a political jurisdiction, i.e., county, state, or country[554]. For an

552 C. Kuner (note 507).

553 Burke T. Ward & Janice C. Sipior, *The Internet Jurisdiction Risk of Cloud Computing*, 27 Information Systems Management 334–339 (2010.)

554 *Id.*

assertion of personal jurisdiction to be valid, it must satisfy the requirements of the 'due process clause'[555] prescribed in the Fifth and Fourteenth Amendments of the US Constitution. Under certain circumstances, a court can exercise personal jurisdiction over non-resident individuals and businesses under the authority of a state long arm statute[556]. Such statutes serve as a "long arm" to reach defendants outside of the geographical jurisdictional boundaries of the court. One such example of long arm jurisdiction would be a Missouri resident being served with a legal process by a California court.

– Sufficient minimum contacts and long arm jurisdiction

Beginning with International Shoe Company v. State of Washington (1945)[557], the US Supreme Court has held that due process requires that it be established that the non-resident defendant has sufficient minimum contacts with the state attempting to exercise jurisdiction[558]. The nature of the contacts has to be such that the exercise of jurisdiction did not offend traditional notions of fair play and substantial justice[559].

---

555 The Fifth and Fourteenth Amendments to the United States Constitution contain a due process clause. Due process refers to the administration of justice, acting as a safeguard from arbitrary denials of life, liberty, or property by the Government. The Supreme Court of the United States has adopted even broader interpretations of the clauses, which, as it is has found, provide four protections: procedural due process (in civil and criminal proceedings), substantive due process, a prohibition against vague laws, and, lastly, act as the vehicle for the incorporation of the Bill of Rights. Due process, in other words, ensures the rights and equality of all citizens.

556 Long-arm statute is one that allows for a state court to obtain personal jurisdiction over an out-of-state defendant on the basis of certain acts committed by an out-of-state defendant, provided that the defendant has a sufficient connection with the state.

557 International Shoe Co. v. Washington, 326 U.S. 310, 66 S. Ct. 154, 90 L. Ed. 95 (1945.)

558 Burke T. Ward & Janice C. Sipior (note 553.)

559 'Fair play and substantial justice' notion: a requirement or standard of fairness that must be made by a court's assertion of personal jurisdiction over a nonresident defendant in order to sufficiently deter a violation of the defendant's right to due process.
In International Shoe Co. v. Washington, the Supreme Court held that 'in order for a state court to exercise jurisdiction over a defendant whose residence is elsewhere, the court must establish that the defendant has such minimum contacts with the state that the exercise of jurisdiction over the defendant does not offend traditional notions of fair play and substantial justice'. The main factors used to make this determination are:

The minimum contacts standard[560] necessitates at least some physical presence prior to determining jurisdiction. In commercial transactions, the minimum contacts standard has been found to be met, in general, by the presence of a store, warehouse, salesperson, agent, or physical presence[561]. An example of a transaction is the execution of a sales contract; an example of an occurrence is an automobile accident. Overall, a long arm statute gives jurisdictional statutory authority to a local court to hear a case and make a judgment against an out-of-state defendant.

– Long arm statutes to assert internet jurisdiction

The development of the internet has spurred a series of US States to enact long arm statutes enabling them to assert jurisdiction over defendants who take part in e-commerce or other internet activities[562]. One of the oldest such instances, nearly a decade ago, is Georgia's Computer Systems Protection Act, which contains rules for authorizing jurisdiction over computer related crimes[563]. The act stipulates that Georgia will have jurisdiction over an out-of-state defendant 'in any county for which, to which or through which any use of a computer or a computer network was made, whether by wires, electromagnetic waves, microwaves or any other means of communication'[564]. The said statute had been met with certain reservations by its opponents; the most important among the arguments[565] was that the act was viewed as an attempt to regulate interstate commerce and violate the dormant commerce clause[566]. The dormant commerce clause prohibits states from unduly burdening interstate commerce. Their argu-

---

i. the difficulty for the defendant of appearing in the court
ii. the state's interest in deciding the case
iii. the plaintiff's interest in the convenience of the court
iv. the effectiveness of the relief to be obtained there.

560 'Minimum contacts' is a term used in the United States law of civil procedure to determine when it is appropriate for a court in one state to assert personal jurisdiction over a defendant from another state.

561 *Id.*

562 *Id.*

563 Georgia Computer Systems Protection Act, H. B. No. 822 (available under http://www.oit.gatech.edu/georgia-computer-systems-protection-act; date of last access: 19/2/2016.)

564 Id.

565 *Id.*

566 The "dormant commerce clause", also known as the "negative commerce clause", is a legal doctrine that courts in the United States have formulated out of the commerce clause in Article I of the United States Constitution. The commerce

ment is based on prior Supreme Court decisions where the Court invalidated statutes that attempted to regulate interstate commerce or violated the dormant commerce clause[567]. Since then, a lot more statutes of similar nature have been set up by US states in their effort to claim jurisdiction and exert power over the complex issues instigated by the online world and its facilitating technologies.

ii. Jurisdiction under the influence of technological evolution; practices for alleviating jurisdiction risks in the US and internationally over IT-related cases

As technology changes and evolutions in IT, in particular, impact society, laws are forced to live up to the demands of these changes. These adjustments of laws to the new reality are accomplished through amended legislation, judicial decisions, or both. Similarly, US law has moved to respond to these challenges and the new questions they raise over the issue of jurisdiction not only via enactment of new laws that have moved their focus from physical presence to the economics and effects of the commercial activity[568]. In part, this evolution was also brought about by a series of cases involving mail order vendors; yet, it did not result in an absolute jurisdictional standard for e-commerce[569]. These precedent cases are used in courts for bolstering a still fervent argumentation regarding jurisdiction.

---

clause expressly grants to the US Congress the power to regulate commerce "among the several states." Conversely, the dormant commerce clause expresses the idea that this grant of power implies the opposite power — i.e., a restriction deterring a state from passing laws that would improperly burden or introduce discrimination practices against interstate commerce. This restriction is self-executing and immediately applicable even in the absence of a conflict between state and federal statutes, but Congress may allow states to pass legislation that would otherwise be forbidden by the dormant commerce clause.

567 *Id.*

568 *Id.*

569 An indicative list of such cases brought out by US courts would include:
i. Bensusan Restaurant Corp. v. King, 1996; Federal District Court for the Southern District of New York denied jurisdiction by focusing on the local nature of the alleged infringing activity (Bensusan Restaurant Corp. v. King, 1996; Manolopoulos, 2003)
ii. Zippo Mfg. Co. v. Zippo DotCom, Inc., 1997; Federal District Court for the Western District of Pennsylvania determined jurisdiction on a "passive vs. ac-

In the end, no conclusive answer exists yet as to how to address the jurisdiction risk posed by the most up-to-date IT tools, cloud computing in particular. On the contrary, US laws are far from offering a tried and settled test as to determine how to exert jurisdiction on the internet in the US or internationally[570]. The majority of US scholarly opinion maintains the position that the cloud is inherently global, calling for a cross-jurisdictional solution[571]. On the other hand, cloud computing providers systematically seek to reduce liability by proposing cloud service agreements with "as is" provisions[572] and no warranty[573]. This means that most cloud services are provided without any assurance or promise of a specific level of performance. In response, businesses, for the moment and until the issue of jurisdictional rules regarding the cloud is settled, prior to adopting cloud computing need to consider internet jurisdiction risk, as well as other legal issues[574], before deploying a cloud service. The most important criteria against which a cloud service needs to be evaluated before it is adopted or rejected by a business, and which ideally should be assessed both in their virtual and physical dimensions are currently regarded to be[575]:

---

tive" or "sliding scale" test, cited as precedent in many subsequent cases (Geist, 2001; Hestermeyer, 2006; Manolopoulos, 2003; Minnesota v. Granite Gate Resorts, Inc., 1997; Rosenthal, 2003; Rustad & Koenig, 2006; Waldmeir, 2003; Ware, 2006; Zippo Mfg. Co. v. Zippo Dot Com, Inc., 1997)

iii. People Solutions, Inc. v. People Solutions, Inc., 2000; Federal District Court for the Northern District of Texas held that personal jurisdiction should not be based on the mere possibility that it is possible to do business (People Solutions, Inc. v. People Solutions, Inc., 2000).

570 Joel Reidenberg (note 474).

571 Michael R. Nelson, *The Cloud, the Crowd, and Public Policy*, 25 Issues in science and technology 71–76 (2009.)

572 "As is" is a term used in contract law to disclaim some implied warranties for an item being sold. "As is" denotes that the seller is selling, and the buyer is buying an item or server in whatever condition it is at the time the buy is effected, while the buyer is accepting the item "with all faults", whether or not immediately apparent. An "as is" contract puts the buyer in a situation described as the "buyer beware" status, in which buyer is advised to take the time to examine the item or service before accepting it or to ask expert advice for this assessment.

573 McAlpine C., Weigh Legal Risks of Cloud Computing, available at: http://www.baselinemag.com/c/a/Legal/Weigh-Legal-Risks-of-Cloud-Computing-869422 (19 February 2016.)

574 See also Chapter 7.

575 Burke T. Ward & Janice C. Sipior (note 553).

– considering how serious the jurisdiction risk is when compared to a company's corporate strategy;
– establishing a governance structure tackling cloud computing particularities across the enterprise;
– determining the appropriate cloud computing model before selecting a service, i.e. picking a service which complies with the company's adopted cloud protocols;
– partnering with the cloud provider instead of simply subscribing to its services in order to secure an, as much as possible, customized service; and
– securing adequate liability insurance that will keep them immune, to a certain degree, against the financial exposure of internet liability.

g. Corporate strategy as a pre-emptive measure for facing the long arm of cloud jurisdiction

As a rule, businesses maintain that they should comply with the laws of all countries in which they conduct business and avoid violating laws in countries in which they do not do business[576] but in which their facilities, applications or the data they handle physically reside. Consequently, this global legal environment which, however, is contradicted by the fragmented landscape of different legal orders, demands that modern businesses' corporate strategies directly address jurisdiction risk both on its virtual and physical dimensions[577]. In the end, proper evaluation of jurisdictional implications has become a de facto and constant managerial activity, at least until the jurisdictional hurdles the cloud poses are effectively tackled by law.

i. Virtual and physical environments

The overall behavior of businesses towards cloud computing need also take into account the double nature, which is almost inherent to all kinds of cloud-related business making[578]. That is to imply that businesses uti-

576 *Id.*
577 Reidenberg, J. R., Schwartz, P. M. (note 174); Reinhard Posch (note 240).
578 Burke T. Ward & Janice C. Sipior (note 553).

lizing the cloud almost unanimously operate in two environments, the virtual, and the physical ones[579]. These two may be regarded as separate and distinct; however, corporate strategy must comprehensively address legal issues raised by both of them[580].

ii. Accepting the inherent nature of cloud jurisdiction risk

In conclusion, it is evident from the examination that has been carried out that, under the present status quo of US laws, the jurisdiction risk associated with cloud computing is continuous and inherent. Therefore, businesses are advised to maintain corporate strategies that steadily look for ways to reduce this risk. The practical way to achieve this is by conducting a detailed legal analysis and assessment of those risks across different countries and multiple jurisdictions, certainly in those which are relevant for each undertaking (i.e. the legal order where the company resides, where it has its data storage facilities or where its services are accessible etc.).

Based on this constant monitoring mechanisms, the governing body of a business is expected to make conscious and deliberate decisions or adaptations thereof as to where and how cloud computing processes of the enterprise are conducted. These strategic decisions are made and reviewed based on criteria such as a company's capabilities and resources, knowledge base, applicable domestic and foreign laws and perceptions of risk in conducting business activities[581].

h. Where are cloud data centers located? How jurisdiction plays a major part in deciding on geographic location, economic and environmental parameters in cloud computing

Having examined how Europe and the US treat the issue of determining jurisdiction over cloud computing, it is worth briefly summarizing how the above practices bear real effect on the actual cloud computing business. Essentially, what makes cloud computing possible is the data centers

579 Robert Ware, *The strategic use of American cyberlaw and cyberspace jurisprudence*, 48 Managerial Law 303–321 (2006.)
580 Burke T. Ward & Janice C. Sipior (note 553).
581 Robert Ware (note 579).

where data of the users of various services are hosted and which provide the resources necessary for the execution of any processing tasks involving that data. Anyone who is interested in setting up a data center that will offer services based on cloud computing technologies and protocols evaluates the following four primary considerations of where in order to choose where their data center will be constructed[582]:

– Suitable physical space in which the warehouse–sized buildings that will host the data center's hardware will be located
– Proximity to high–capacity Internet connections
– The availability of affordable electricity or other energy resources
– The laws, policies, and regulations of the local jurisdiction

Interestingly but not surprisingly, one of the major factors weighing decisively on the decision regarding the location of cloud computing data centers is the jurisdictional issues that the chosen location will give rise to. As it has already been sufficiently demonstrated, the laws, policies, and regulations of a particular jurisdiction can have a significant impact both on the cloud provider and the cloud user. Governments and legislators can either stifle or promote the development of cloud computing within a particular jurisdiction with the decisions they are empowered to make and the laws they can enact on the topic.

We have already examined the main challenges the issue of jurisdiction raises with regard to doing business in the field of cloud computing. Similarly, numerous and equally gravitational law and policy concerns exist also for cloud users as a result of the jurisdiction risk associated to the cloud[583]. For users, the most crucial of these issues and expectations include[584]:

– Access: users expect to be able to access and use the cloud where and when they wish without any hindrance from the cloud provider or third parties.
– Reliability: users expect the cloud to be a reliable resource, especially if they assign to their cloud provider tasks that are of a critical nature to their business or online presence, in general.

---

582 Paul T. Jaeger, Jimmy Lin, Justin M. Grimes & Shannon N. Simmons (note 208).
583 Paul T. Jaeger, Jimmy Lin & Justin M. Grimes, *Cloud Computing and Information Policy: Computing in a Policy Cloud?*, 5 Journal of Information Technology & Politics 269–283 (2008.)
584 Paul T. Jaeger, Jimmy Lin, Justin M. Grimes & Shannon N. Simmons (note 208).

- Security: users expect that the cloud provider will not allow unauthorized access to both data and code, and that these will remain secure at all times.
- Data confidentiality and privacy: users expect that their cloud provider, other third parties, and governments will not monitor their activities, with the exception of cloud providers selectively monitoring usage for quality control purposes.
- Liability: users expect clear delineation of liability if serious problems occur.
- Intellectual property: users and third party content providers expect that their intellectual property rights will be upheld.
- Ownership of data: users expect to be able regulate and control the information that is created and modified using the cloud services they have chosen.
- Portability: users expect that data and resources stored in one cloud facility can be easily moved or transferred to another facility or service with little or no effort.
- Auditability: users, particularly corporate, expect that providers will comply with regulations or at least be able to provide them the option to have them audited per regulation requirements.

PART II: Accountability on the cloud

a. Accountability: the essentials from data protection to cloud computing

Having discussed the issue of how to claim jurisdiction over cases seeking judicial resolution in the field of cloud computing and the broader area of IT law, it is now time to look on the other side of the coin. Besides establishing rules that answer the question what court or jurisdiction is competent to adjudicate on a case, immediately afterwards comes the question of who is to be held responsible about that case.

In the most up-to-date fields of human activity, the term used to refer to this responsibility about an act or incident is 'accountability'[585]. The term

585 Siani Pearson & Andrew Charlesworth, *Accountability as a Way Forward for Privacy Protection in the Cloud*, in Cloud computing. First international conference, CloudCom 2009, Beijing, China, December 1-4, 2009 : proceedings, 131–144 (Martin Gilje Jaatun, Gansen Zhao & Chunming Rong eds., 2009.)

is anything but new but recently it has been coined with several meanings: from an ethics and governance point of view (stricto sensu accountability), accountability is implied as answerability, liability, and, of course, as the respective expectation of account-giving[586]. Viewed as a sub-sector of governance (lato sensu accountability, accountability has been associated with issues in public, nonprofit as well as private (corporate) sector, even within individual contexts[587].

In recent governance theories, accountability has expanded beyond the basic concept of "being called to account for one's actions"[588]. Several researchers have brought forward a description of accountability as a relationship, an at least two-party structure with account-giving between its constituents at its core[589]. In an illustrative manner, accountability is the bond between actor A and actor B when "A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct"[590].

It goes without saying that, as a tracking and reporting mechanism, accountability cannot function without proper accounting practices and mechanisms; in other words, an absence of an accounting workflow automatically means an absence of accountability[591]. On a generic level, the essential elements for a solid accountability policy are[592]:

– commitment of the organization adopting accountability to the main principles of it and adoption of internal policies consistent with external criteria.
– mechanisms that will put privacy policies into effect, such as relevant tools, training and education.

---

586 Clarence A. Dykstra, *The Quest for Responsibility*, 33 The American Political Science Review 1–25 (1939.)
587 M. Bovens, The Quest for Responsibility: Accountability and Citizenship in Complex Organisations (1998.)
588 Richard Mulgan, *'Accountability'. An Ever-Expanding Concept?*, 78 Public Administration 555–573 (2000.)
589 Andrew Charlesworth (note 185).
590 Andreas Schedler, Larry Jay Diamond & Marc F. Plattner, The self-restraining state. Power and accountability in new democracies (1999.)
591 Siani Pearson & Andrew Charlesworth (note 585).
592 Centre for Information Policy Leadership, Data Protection Accountability: The Essential Elements A Document for Discussion, available at: http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (19 March 2015.)

– systems enabling constant oversight internally, towards collecting the data necessary for regular assurance reviews and, eventually, external verification.
– transparency and mechanisms facilitating individual participation in the accountability process.
– means for remediation and external enforcement.

Accountability in the broad field of data management and protection is designed with a view to make some strong protection processes for data possible[593]. Where implemented, accountability allows the said organization much more extensive flexibility to adapt its data practices[594]. Of course, in order for it to function properly and efficiently, it requires that the organization commit to and actively demonstrate its upholding of responsible policies and of systems necessary to ensure those policies are carried out in a manner that protects information and the individuals to which it belongs or refers[595]. In other words, accountability as a governance practice, requires that an organization remains accountable no matter where the information it handles is processed. Functioning under the prism of accountability, a data-related organization is less interested in the rules that exist where the data is processed and more in those applicable where the obligation is first established[596]. That said, it becomes evident that data management accountability is purpose oriented and constructed based on a teleological perspective, putting emphasis not on when and where a breach occurred but rather on who had the obligation to take every measure possible to prevent the breach from happening based on their position and role in the data cycle.

b. Accountability is not self-regulation; clearing the picture between two comparable but critically different concepts

Having described the nature and content of the term 'accountability' (stricto and lato sensu), it is vital to clear an ambiguity as to what account-

593 *Id.*
594 David R. Johnson, Susan P. Crawford & John G. Palfrey, *The accountable net: Peer production of internet governance*, 9 Berkman Center for Internet & Society at Harvard Law School Virginia Journal of Law and Technology 1–32 (2004.)
595 *Id.*
596 Siani Pearson & Andrew Charlesworth (note 585).

ability in the cloud would be in essence. There has been a considerable share of scholars and industry experts who have been equating accountability in cloud computing with the self-regulation structure the industry and policy actors devised in order to regulate internet names and numbers in the second half of the 1990s[597]. The model of ICANN[598] was a response to the need for effective internet governance and involved creating an entirely new institutional and property rights framework[599]. At its core lied the problem of who owned probably the most important, valuable assets of the internet, i.e. the name and address spaces[600]. Under the ICANN scheme, control of these assets was voluntarily transferred from an informal set of competent agencies loosely belonging to the US government and its private contractors to a formal, internationally representative, legally incorporated entity[601]. As a result of this 'migration' a whole range of sophisticated property rights issues came up[602]. ICANN, as an organization and as a structure, had to cope with as challenging issues as how to reconcile domain name registration with trademark protection, what rules or procedures governing access to the root of the domain name space would be, how much control a domain name registry would have over the zone files containing the authoritative list of second-level names and many more[603]. These questions, purely legal in nature, were even further complicated by the global, trans-jurisdictional scope of the system. Ultimately, the US Department of Commerce gave answer to these issues by basically devolving global state power to ICANN[604].

---

597 Milton Mueller, *ICANN and Internet governance: sorting through the debris of "self-regulation"*, 1 info 497–520 (1999.)

598 ICANN (Internet Corporation for Assigned Names and Numbers) is a nonprofit organization, organized from the Secretary of State of the State of California in the U.S. that is responsible for coordinating the maintenance and methodologies of several databases, with unique identifiers, related to the namespaces of the Internet – and thereby, ensuring the network's stable and secure operation. ("ICANN Bylaws", 30 July 2014. Retrieved 30 June 2017.)

599 *Id.*

600 Jonathan G. S. Koppell, *Pathologies of Accountability*. *ICANN and the Challenge of "Multiple Accountabilities Disorder"*, 65 Public Administration Review 94–108 (2005.)

601 Milton Mueller (note 597).

602 *Id.*

603 Jonathan G. S. Koppell (note 600).

604 Milton Mueller (note 597).

This enormous venture of self-regulation seems comparable but is definitely not identical to the concept of accountability[605] that has been previously discussed and is put forward as a way to achieve pragmatic cloud computing regulation. The harmonization reached via ICANN was based on the strong motives given to the market to seize control of the process and the property rights issues that stemmed from it and, more or less, to try and win in a struggle for power[606]. Accountability, on the other hand, is not about deciding who among market factors will retain more power over the others but, rather, about putting in place a governing scheme that will clearly delineate roles for the actors of the cloud computing sphere, describe their rights and duties, what function(s) they are expected to fulfil across the cloud computing cycle and what kind of responsibility they carry as a result of only partially or wrongly fulfilling those functions. In other words, accountability is not an initiative left entirely to the good will of private sector[607]. It is a two-level process whereby, on the one hand, the legislator and the empowered inspecting authorities make sure a set of rules and regulations is upheld and, on the other hand, private actors – stakeholders of the cloud market – self-adhere to those rules a priori and not only when a breach is found to have been committed from them[608]. In other words, for accountability to bear fruit, a pre-emptive rather than a punitive logic is necessary.

c. Accountability in the cloud cannot be sufficiently settled with existing EU laws

The way relevant EU legislation has been constructed until today, does not offer an adequate scheme that would effectively govern cloud computing from the perspective of accountability and not merely culpability, as it has been happening so far. There are primarily two main proposals that merit serious consideration in order for the EU regulatory thinking to be in a position to offer realistic solutions in the challenges posed by cloud tech-

605 Marcel Machill, Thomas Hart & Bettina Kaltenhäuser, *Structural development of Internet self-regulation*, 4 INFO 39–55 (2002.)
606 Milton Mueller (note 597).
607 Marcel Machill, Thomas Hart & Bettina Kaltenhäuser (note 605).
608 *Id.*

nologies[609]. Firstly, the binary distinction between controllers and processors, sitting right now at the heart of the regulatory scheme utilized to decide on cloud-related issues, is unsuitable for a cloud computing environment and should be abolished[610]. Alternatively, a wholly new principle of end to end accountability needs to be introduced, one that would run through the cloud business chain and will at all times hold the different actors accountable for their share of duties in the broader task of making sure the cloud cycle runs smoothly. Secondly, in order to strike a finer balance between protection of privacy and the fostering and further growth of the cloud sector and business, it is suggested to introduce in the cloud industry a logic already present in other pieces of EU legislation about similar matter, for instance, in the Privacy and Electronic Communications Directive[611]: in particular, it is high time to start thinking whether it makes sense for pure infrastructure cloud providers to be treated as neutral intermediaries, unless and until they have the requisite knowledge and control over a specific bunch of data (in the form of access to it, at least for more than incidental purposes). In this way, the industry will benefit, on the one hand, from not having to bear the burden of a constant suspicion in case a breach occurs at some point over the cloud computing cycle. At the same time, by setting aside infrastructure as a prima facie reason for breaches of the cloud cycle, we profit from not sticking to a convenient and obvious answer but focusing instead on the actual actors of the cloud computing business that could, due to their role and the processes they execute, cause a harmful incident involving certain volumes of data and their owners or subjects.

In detail, after doing away with the simplistic binary controller/processor distinction, it is suggested that the cloud industry be reorganized based on an end to end accountability approach[612]. This approach will lead the greater sector to be arranged over a continuum or spectrum of parties, of whom only those that indeed process data at some point through the data life cycle will be considered as potentially culpable. Additionally, this ac-

609 Siani Pearson & Andrew Charlesworth (note 585).

610 J. Domingue, D. Fensel & J. A. Hendler, Handbook of Semantic Web Technologies (2011.)

611 Martin Gilje Jaatun, Gansen Zhao & Chunming Rong eds., Cloud computing. First international conference, CloudCom 2009, Beijing, China, December 1-4, 2009 : proceedings, vol. 5931 (2009.)

612 David R. Johnson, Susan P. Crawford & John G. Palfrey (note 594).

countability will not be vague nor will it only be affirmed when a wrongdoing occurs[613]. It will, instead, have varying degrees of obligations and liabilities, directly analogous to the position of the party in the cloud cycle, the scope it is supposed to be serving and the processes for which it is fair to be held responsible[614]. This approach would not only bring the actual responsible parties to the forefront of culpability but it would also contribute to the quest for achieving a more appropriate balance between commercial and privacy considerations in light of the complex and dynamic nature of today's cloud computing industry.

d. Providing answers to the privacy challenges of cloud computing under US law; the importance of the Fourth Amendment principles

In general, we are used to be regarding the US as a legal culture with not as much preoccupation about privacy as Europe. While that might have been true until recently, things have rapidly been changing especially under the effect of events of considerable magnitude, such as the Snowden scandal and other threats or direct intrusions to citizens' privacy that have come to light as of late. The origins of the quest for protection of privacy in the American legal culture are found in a landmark decision of the US Supreme Court, Katz v. United States[615]. The case was a chance for the US Supreme Court to revisit its stance on the basic principles of the Fourth Amendment of the US Constitution[616]. In the same decision, the

613 *Id.*

614 Andrew Charlesworth (note 185).

615 Katz v. United States, 389 U.S. 347 (1967): in this United States Supreme Court case the nature of the "right to privacy" and the legal definition of a "search" were extensively discussed and profoundly updated to mirror modern challenges. The Court in its ruling refined previous interpretations of the unreasonable search and seizure clause of the Fourth Amendment to also include immaterial intrusion with technology as a search, overruling previous decisions, i.e. Olmstead v. United States and Goldman v. United States, that had adopted more restrictive views on the matter. In Katz, the US Supreme Court also extended Fourth Amendment protection to all areas where a person has a "reasonable expectation of privacy".

616 The Fourth Amendment of the U.S. Constitution reads, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

US Court put also forward the 'reasonable expectation of privacy test'[617]; with regards to it, one of the concurring judges, Justice Harlan, outlined a two-fold requirement for the call for protection to be justified; that the person demonstrated a subjective expectation of privacy over the object and that the expectation was reasonable[618].

The focus of the analysis regarding the reasonable expectation of privacy in Katz was on how courts generally define searches of containers under the Fourth Amendment[619]. Nevertheless, the same decision also stood for another important principle of Fourth Amendment jurisprudence: that "the Fourth Amendment protects people, not places."[620] As a result, this decision marked for the first time a shift of focus in US legal thinking from "persons, houses, papers, and effects,[621]" which are the spaces or areas where the Fourth Amendment principles directly apply to, towards a broader view which extended protection to privacy interests in intangible communications[622].

This novel approach to protection of privacy has to be once more updated today to give meaningful responses to the issue of intangible digital data, their handling and the main tools for processing them, such as cloud computing[623]. Although computers and the devices or technologies prevailing in today's IT sector are more technologically complex than brief-

---

probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
The ultimate goal of this provision is to protect people's right to privacy and freedom from arbitrary governmental interventions. Private intrusions not acting in the color of governmental authority were exempted from the Fourth Amendment at the time of its adoption.

617 The reasonable expectation of privacy is a legal test essential in defining the scope of the applicability of the privacy protections of the Fourth Amendment to the United States Constitution. The test is essentially related but not the identical to the 'right to privacy', which is a much broader concept central to EU law and many other legal systems that have developed under EU law influence.

618 Katz v. United States (note 615.)

619 DAvid Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minnesota Law Review 2205–2239 (2009.)

620 Katz v. United States (note 615.)

621 U.S. Constitution, amend. IV.

622 *Id.*

623 D. Scott Blake, *Let's Be Reasonable: Fourth Amendment Principles in the Digital Age*, 5 SEVENTH CIRCUIT REV. 491–531 (2010.)

cases or even perhaps telephone calls, US courts have already held that computer searches are limited by the Fourth Amendment[624].

There have already been instances where courts have extended the protective legal structure which has its origins in the Katz case into the cloud computing world[625]. In particular, the district court in D'Andrea case[626] recognized that virtual containers do exist in the cloud, hence protection of privacy is a legitimate request also in the realm of cloud computing. However, legal scholars still believe that the US justice needs to take further steps in order not just to recognize the legitimacy of the call for privacy protection on the cloud but also to legitimize certain types of tools that will facilitate the fulfilment of this call[627]. Consequently, there have been voices calling upon US justice to also acknowledge the legitimacy of virtual concealment efforts, namely, encryption, password protection, and the practical obscurity of unlisted links, as means of opacity in the cloud context[628]. It is suggested that if these steps were taken, courts would then be in a position to make a case-by-case determination as to whether a user's behavior online or his recourse to tools such as passwords, encryption, or obscurity techniques were reasonable in a given situation or went beyond legitimate[629]. On the other hand, this delineation of what is permissible and what is not in the cloud environment, will also boost the previously discussed call for accountability over culpability in the cloud. Consequently, while maintaining its distinct position from other jurisdictions, the US

624 For example, in Maes v. Folberg, 504 F. Supp. 2d 339, 347 (N.D. Ill. 2007), an Illinois federal district court found that the plaintiff, a state employee, had a reasonable expectation of privacy in her government-issued laptop computer because there was no evidence that the plaintiff was on notice that her laptop was subject to search. The court relied upon O'Connor v. Ortega, which held that government employees are protected from unreasonable searches by their government employers. Maes, 504 F. Supp. 2d at 347–48 [citing O'Connor v. Ortega, 480 U.S. 709, 715–16, 725–26 (1987)]; cf. Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (holding that plaintiff's privacy expectation was destroyed because his government employer "announced that it could inspect the laptops that it furnished for the use of its employees").

625 David Couillard (note 619).

626 United States v. D'Andrea, 648 F.3d 1 (1st Cir. 2011.)

627 D. Scott Blake (note 623).

628 S. S. Smith, Web-based Instruction: A Guide for Libraries (2006); David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 Connecticut Law Review (2017.)

629 Jack L. Goldsmith & Tim Wu (note 535).

legal system can also take steps towards harmonization of the universal legal landscape regarding cloud computing regulation.

e. Achieving effective regulation of the cyberspace: discussing particularities of the web and how these should be mirrored in modern laws about aspects of the digital world

In every matter calling for regulation, the ultimate aim of policymakers has always been to strike a balance between protecting the rights of the parties affected by the legislation, on the one hand, and the constraints that need to be introduced for the enjoyment of these rights not to create conflicts between different law subjects, on the other[630]. For example, in the field of intellectual property law, the aim of policymakers is to strike a balance between securing some protection for creators for their work while ensuring that that protection does not reach so far as to pose conflicting situations.

The same challenging balance has to be struck in the field of privacy. Every free society believes that there is some realm of individual life that should be free of surveillance or invasion[631]. Among societal factors, there are those who are strong promoters of this privacy realm, which they believe that sits beyond government regulation. There are, of course, other more moderate voices who assert that this realm at least should be presumptively free from state control. Opposite all these sit the policymakers who need to fine tune all tendencies into an efficient regulatory scheme[632].

The question that comes naturally to mind is how policymakers achieve this balance and what factors they need to take into account when designing laws. The traditional school of thought in legal science supports that in designing a law only those factors directly tied to the subject matter that is

630 Lawrence Lessig (note 505).

631 This view is documented, for example, in Lawrence v. Texas, 123 S. Ct. 2472, 2475 (2003). Justice Kennedy wrote: Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition, the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct.

632 *Id.*

to be regulated need to be considered[633]. Consequently, in long-established fields of law, such as intellectual property, the balance is achieved by considering the sum of statutory and common law protections. Similarly, a fair statutory scheme for privacy protection takes into account the same kind of protections, as well as the constitutional perspective[634]. In other words, from the traditionalists' perspective policymaking is simply the process of tuning legal code[635]. Any changes in policy, from this point of view, simply map changes in legal code[636].

Nonetheless, as it has become clear already, when it comes to regulating aspects of the cyber world and its enabling technologies, policy making cannot be done solely based on legal code[637]. Instead, it is essential to maintain a continuous interaction between the legal code and the architecture or technology within which this code will be called to function on every occasion, i.e. in every different phase of technological status quo[638]. This applies to virtually all aspects of the internet, such as privacy and, of course, now cloud computing. In its early days, the Internet, its architecture and its technologies produced relative anonymity for users[639]. The very first internet protocols were neither designed for nor based on recognizing who people were, where they came from, or what use they were making of the Internet[640]. That information, back in the time, was not embedded in the basic Internet protocol, which meant that the basic protocols protected users from inadvertent releases of such information. Consequently, the balance between privacy and respect for the user's fundamental rights and, on the other hand, the interests of those doing business on or for the internet was much easier to strike. However, things have rapidly changed today, with a great deal of internet services and applications being based on the personalization of the work environment or the tying of the service to each and every individual user[641]. In view of these, the bal-

633 *Id.*
634 Paul Schiff Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to 'Private' Regulation*, 71 University of Colorado Law Review 1263–1310 (2000.)
635 L. Lessig (note 504).
636 *Id.*
637 *Id.*
638 Joel Reidenberg (note 474).
639 L. Lessig (note 504).
640 *Id.*
641 See Chapter 2.

ance policymakers have to achieve between conflicting tendencies and interests of the internet sphere actors has become all the more precarious.

As of late, there have been increasingly louder voices arguing that the best way to make the internet and its surrounding ecosystem, including cloud computing, flourish is to limit or refrain from regulation of it, giving it the chance to self-regulate itself[642]. Much as it is supposed to support a liberal take on cyberspace, this unwillingness to regulate eventually defeats the very values that is supposed to be defending[643]. It should not be overlooked that, all the more so after the recent developments regarding internet security around the world, citizens and a big share of the internet stakeholders in general, voice stronger and stronger calls for a more efficiently regulated virtual world[644]. In other words, the answer to the particular nature of the internet, which decisively affects its regulatory needs, is not to go from the extreme of overregulation to that of non-regulation.

It is not the first time that the law will need to work hand in hand with other sectors in order to provide efficient answers to novel challenges[645]. A spirit of openness is necessary. As many are beginning to recognize, probably the most salient feature of cyberspace is its ability to embed controls that resist or reinforce values that we bring to it[646]. This capacity is a unique asset in designing and implementing effective laws for the cyber world and its constituting parts, i.e. also for cloud computing. Understanding the manner in which these values are resisted or reinforced will allow us to design a regulatory scheme that will promote accountability while, at the same time, will make cloud computing and all the areas where it is used more user-friendly and less of a mystery, boosting its prospects as a business sector as well.

642 Chris Reed (note 363).
643 Lawrence Lessig (note 505).
644 See also Chapter 3.
645 Siani Pearson & Nick Wainwright, *An interdisciplinary approach to accountability for future internet service provision*, 1 IJTMCC 52–72 (2013.)
646 Lawrence Lessig (note 505).

f. Tackling the issue of perspective in internet law; an essential step towards a pragmatic accountability regime

Law, in doctrine and in practice, can be understood from either an internal or external perspective[647]. The internal perspective is the one adopted by judges and lawyers who work within the legal system. In their official function, these actors of the law cycle are required to view the law as a set of rules with legitimacy and moral authority[648]. On the contrary, the external perspective is predominant among sociologists, economists, and historians, i.e. experts who approach law and legal conduct as epiphenomenal, as a reflection of deeper forces unrecognized by the players within the law cycle[649]. Simply put, the internal perspective approximates a first-person view or insider's view of the legal system, whereas the external perspective is a third-person view or observer's view of the law[650].

The problem of perspective is also present in Internet law and how this is resolved will largely determine the nature and shape of regulation that will be set in place to regulate the internet and, consequently, cloud computing. Experience proves that in a surprising number of situations, the outcome reached when applying law to one case from an internal or an external perspective is profoundly different[651]. The cyber space and its subdomains or enabling technologies are a prime example of such fields where major regulatory challenges essentially boil down to clashes between the internal and external perspective[652]. To further complicate matters, neither perspective is a priori right or wrong, nor is any of the two more or less legitimate. Both perspectives can prove to be perfectly viable depending on the circumstances; therefore, courts and commentators switch between them frequently without even recognizing the change[653].

The essential task of a regulator is to apply legal rules to facts and reach meaningful solutions to outstanding conflicts between them[654]. In the case

---

647 E. Douglas Litowitz, *Internal versus external perspectives in law: toward mediation*, 26 Florida State University Law Review 127–150 (1998.)
648 Orin S. Kerr (note 230).
649 E. Douglas Litowitz (note 647); Philip Leith, *The socio-legal context of privacy*, 2 IJC 105–136 (2006.)
650 E. Douglas Litowitz (note 647).
651 Orin S. Kerr (note 230).
652 Paul Schiff Berman (note 634).
653 Orin S. Kerr (note 230).
654 E. Douglas Litowitz (note 647).

of the internet and cloud computing, however, there are two strongly competing understandings of reality. On one side, there is a virtual reality, which is the one we come to view through the internal perspective and, on the other side, there is a physical reality, which we perceive when viewing cloud computing from the external perspective[655]. This brings the regulators (and all other actors involved in cloud governance) before a dilemma as to which perspective should be adopted when attempting to regulate the cloud. By choosing the perspective, we choose the reality; by choosing the reality, we choose the facts; and by choosing the facts, we choose the law[656].

From the internal perspective of cloud users, cloud computing is the work environments of the cloud-based services they are using, and they understand regulating the cloud as the task of projecting real world situations to the virtual world of cyberspace, spotting the analogies between the two and trying to match the rules between them[657]. To external observers, in contrast, cloud computing is the physical infrastructure and the constituting parts of the cloud environment; for them, applying law to the internet means applying the law to the constituting parts that made feasible the operation of the cloud network[658].

A direct 'product' of this ongoing divide between the internal and external perspective in internet law has been the increasingly popular concept of 'internet governance' which has already been discussed[659]. Internet governance can be defined as the study of how law, legal institutions, and computer code collectively regulate and define the virtual world of cyberspace[660]. Internet governance, as a normative structure, has been nourishing from this sharp division along internal and external perceptions of the internet, and this should come as no surprise[661]. In essence, internet governance seeks to expose the analogies between the process of creation

655 Renzo Marchini, Cloud computing. A practical introduction to the legal issues (2010.)
656 Lawrence Lessig (note 505).
657 Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang & Anand Ghalsasi (note 116).
658 *Id.*
659 See Chapter 5.
660 Francesca Musiani & Internet Policy Review, Decentralised internet governance: the case of a 'peer-to-peer cloud' (2014.)
661 David S. Wall, *Digital Realism and the Governance of Spam as Cybercrime*, 10 Eur J Crim Policy Res 309–335 (2004.)

of rules in the physical world (traditional questions of governance) and the creation of rules in cyberspace (internet governance)[662]. Similarly, extended to the issue of cloud computing, a sound governance scheme, which will in turn permit a sound accountability mechanism, strives to identify connectors between the challenges and points of concern of the cloud ecosystem users and actors and the external perceptions held about the cloud by the regulators.

In social sciences, the terms "internal" and "external" are normally used to compare different ways of analyzing a phenomenon such as religion and law. The internal perspective is the view of a participant in the system, who feels bound by its rules; the external perspective is the view of a third-party observer who does not consider himself bound[663].

As far as law is concerned, this bipolar internal vs. external view was famously applied by H.L.A. Hart in The Concept of Law[664]. According to Hart, viewed from the internal perspective, the law as a system holds that we are bound by its rule, and indicates faith in the power and authority of legal reasoning and doctrine. In contrast, when perceiving law externally, legal rules are understood merely as dressing for other forces that generate observable regularities of behavior but have little additional significance[665].

Nevertheless, when it comes to the internet and cloud computing, the two perspectives mirror two different representations of reality[666]. In a nutshell, the external perspective brings to surface physical reality, and the internal perspective exposes virtual reality. For instance, accessing a website on a browser can be interpreted as either sending a request to a remote server that sends back text and pictures (physical reality), or getting access to a place where certain information is hosted (virtual reality). An internal and an external viewer form two strikingly different understandings of the same thing[667]. Of course, there can be users who have an understanding of both realities simultaneously[668]; technically savvy users, with a certain

662 Orin S. Kerr (note 230).
663 Gustavo Ribeiro, *No Need to Toss a Coin: Conflicting Scientific Expert Testimonies and Intellectual Due Process*, 12 Law, Probability and Risk 1–44 (2013.)
664 H. L. A. Hart, The concept of law (1998.)
665 John T. Noonan, *THE CONCEPT OF LAW. By H. L. A. Hart. Oxford: Oxford University Press, 1961. Pp. viii, 263. 21s*, 7 Am. J. Juris. 169–177 (1962.)
666 Orin S. Kerr (note 230).
667 E. Douglas Litowitz (note 647).
668 Orin S. Kerr (note 230).

level of awareness about technology can very efficiently follow the external view along with the internal. Nonetheless, the internet and cloud computing as its main facilitator necessitate a choice between these two representations of reality. A user may be aware of both realities at the same time, but will have to choose to accept only one at a time when trying to understand online experiences. On the contrary, while regulators, alone or with the assistance of specialized advisors, may well be able to distinguish between the two versions of the cloud reality, they cannot act so in extremis as plain users: they need to come up with a set of rules of law which will serve the interests, respond to challenges and, ultimately, strike a balance between both perceptions of the cloud computing phenomenon in order for this law to provide thorough and not partial answers. This is the only way in which the accountability mechanism that will be put in place can work all the way through different stages of the cloud cycle, be objective and essentially universal, even if it will have of course to respect jurisdictional particularities.

g. The road to an accountable cloud computing goes through the road to an accountable internet: how to achieve a sound internet governance

Cloud computing is, without doubt, the main and major facilitator of the internet. And just as we have seen that there is only one internet, there is also only one basic concept of cloud computing. Particular arrangements may change from one facility to the other, specific technical features may be added or blocked or be only partially available from one cloud environment to the other but the general idea of the cloud, the technologies it is based on, the fundamental principles it has been built upon and the functions it is supposed to fulfil are universal and the same regardless of where a cloud facility is located, from where it is accessed or where it gives access to. However, although there is only one internet and only one core concept of cloud computing, there is neither a global system operator nor a global regulator. And even if there were such an operator, it would be in such an advantageous and powerful position that, in the end, it would not be accountable to anyone, let alone the system it ruled over[669]. Even in the extreme case when an election of an online government was possible, the

669 David R. Johnson, Susan P. Crawford & John G. Palfrey (note 594).

only way for it to produce truly uniform laws would be by systematically discriminating against the interests of minorities in a heterogeneous world[670]. However, the key to a genuinely global internet and cloud computing administration is not to cede power over either of these to a central authority. What we need, instead, is to painstakingly describe and commonly agree on the elements that make up the internet and the cloud, as concepts, the actors taking part in the cloud computing network, the role each on them holds in the course of the cloud chain and the responsibilities they carry, or else, the duties they are expected to fulfil. As long as we create this common ground of understanding, each of the regional governing systems or authorities responsible for ruling over the internet or cloud computing across the globe will have a starting point from which to produce laws that will preserve the autonomous character of the jurisdiction from which they originate but, at the same time, will very efficiently interact with each other and produce viable and borderless solutions. As the internet and cloud technologies continue to evolve, new tools that make this interconnectivity even easier and more effective will become available[671]. Along with laws based on a minimum common understanding, technological tools with better and better functionalities will enable us to single out actors on the cloud that uphold or banish others that abuse trust, good will and ethics. In this way, accountability of the internet as a whole will be continuously augmented and, simultaneously, accountability of cloud computing, as the main technology that makes the web possible, will also be continuously improving.

h. Effective accountability for cloud computing

A cornerstone characteristic of the way cloud computing services are organized nowadays is the outsourcing from cloud service providers of non-core aspects of their business to third parties[672]. That, along with the effec-

670 *Id.*

671 Julia Black, *Constructing and contesting legitimacy and accountability in polycentric regulatory regimes*, 2 Regulation & Governance 137–164 (2008.)

672 Siani Pearson & Andrew Charlesworth (note 585).

tively boundless nature of the cloud from a geographical perspective[673] renders the complexity of the service provision ecosystem even greater, even though many times that may not be visible to an individual or business end user[674]. Nevertheless, it is imperative to device a way for each of these links in the cloud cycle to be held accountable, among themselves and to the regulator for how each of them manages, uses, and passes on data and other related information (e.g. metadata)[675].

This chain of accountability, which will be illustrated in detail later on, will allow the members of a cloud ecosystem to ensure that the obligations and specific duties each one undertakes to protect data while they are within the reach of their responsibility are duly observed at all times and uninterruptedly; in this manner, data remain continuously protected by all who process them at any point of the cloud cycle, irrespective of where that processing occurs at each time. Of course, this will not only apply when a data subject will directly use cloud services, but also when such services will be provided in an enterprise cloud setting.

The legal essence behind this concept of a chain of accountability is discussed in Chapter 7 of this study. However, an overview of how and on what principles this cycle will be built can already be described[676]: service providers, implementing accountability mechanisms, will provide users with control and transparency over data in the cloud. The links between them as elements of the chain of accountability should not understood as simply technical linkages; they will be genuine accountability relationships between supplier and customer, embodied in contracts, addressing regulatory obligations, ensuring each partner will use interoperable policies and functioning efficiently and effectively for the supplier and the

673 Mark Gondree & Zachary N.J. Peterson, *Geolocation of data in the cloud*, in the third ACM conference, 25 (Elisa Bertino, Ravi Sandhu, Lujo Bauer & Jaehong Park eds.)

674 Paul T. Jaeger, Jimmy Lin, Justin M. Grimes & Shannon N. Simmons (note 208).

675 Mark Gondree & Zachary N.J. Peterson (note 673).

676 Siani Pearson, Vasilis Tountopoulos, Daniele Catteddu, Mario Sudholt, Refik Molva, Christoph Reich, Simone Fischer-Hubner, Christopher Millard, Volkmar Lotz, Martin Gilje Jaatun, Ronald Leenes, Chunming Rong & Javier Lopez, *Accountability for cloud and other future Internet services*, in 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), 629–632.

service user[677]. Additionally, apart from the overall chain of accountability extending from end to end over the supply chain, shorter, mole localized accountability bonds will also be possible as a result of deployment of accountability-enhancing mechanisms throughout the service network[678].

All the above linking and controlling mechanisms will be made possible also thanks to trusted third-party services, which will offer monitoring, certification, trust modelling and other functionalities that support any accountability structure[679]. All these inherent and third-party accountability tools will, on the one side, enable providers to implement accountability, on the other side will support users in assessing the trustworthiness of each service and, will also offer to governance actors effective ways to check and monitor the use of data in the cloud[680].

i. Accountability as a way to further reinforce privacy in the cloud

Following the discourse we have presented so far, accountability in the cloud can, in the end, be defined as the management of the availability, usability, integrity and security of the data used, stored, or processed on the cloud, and, as a term, it encompasses all processes by which a particular goal – the prevention of harm to the subjects of the data in question – can be achieved[681]. Towards this end, a combination of public law (legislation, regulation), private law (contract), self-regulation and privacy technology uses (system architectures, access controls, machine readable policies) is deployed[682].

Traditional national and international privacy protection approaches, which had been constructed under the heavy influence of public law are characterized today by declining effectiveness as technological develop-

677 Rolf H. Weber, *Accountability in the Internet of Things*, 27 Computer Law & Security Review 133–138 (2011.)
678 *Id.*
679 Centre for Information Policy Leadership (note 592).
680 Siani Pearson, Vasilis Tountopoulos, Daniele Catteddu, Mario Sudholt, Refik Molva, Christoph Reich, Simone Fischer-Hubner, Christopher Millard, Volkmar Lotz, Martin Gilje Jaatun, Ronald Leenes, Chunming Rong & Javier Lopez (note 676).
681 IEEE ed., An audit logic for accountability (2005.)
682 Siani Pearson & Andrew Charlesworth (note 585).

ments render the underlying regulatory techniques obsolete[683]. In view of the above, the solution towards achieving a viably regulated cloud computing and, in general, IT technologies landscape is that of accountability. What is particularly suggested is a holistic approach combining private and public accountability[684]. Public accountability is made possible thanks to an active interaction between subjects of PII[685], regulatory bodies, such as data Commissioners and data controllers and it is dependent upon highly transparent processes[686]. Private accountability, on the other hand, is made possible thanks to the interaction between data controllers and data processors, and is founded on contract law, technological processes, and practical internal compliance requirements[687]. Along with the change from traditional legal structures to the regime of accountability comes also a shift of focus regarding the way in which the integrity of a cloud network and of the data hosted therein is meant to be achieved. In fact, accountability is not based on setting up extensive procedural or bureaucratic requirements for processing activities but rather on reducing the risk of (disproportionate in context) harm to the subjects of PII and, consequently, on reducing the amount of negative consequences for the data controller[688]. The decisive differentiating point between the previous and the newly proposed status quo is the acceptance that absolute avoidance of harm is an impossible goal in a disaggregated environment, such as a cloud service[689]. Therefore, focusing on enhancing the ability to respond flexibly and efficiently to harm that occasionally arise will provide a more efficient form of privacy protection than the enforcement of blunt compliance criteria.

---

683 L. A. Bygrave (note 137).

684 Siani Pearson & Andrew Charlesworth (note 585).

685 Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

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

687 *Id.*

688 Siani Pearson & Andrew Charlesworth (note 585).

689 Fa-Chang Cheng & Wen-Hsing Lai, *The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy*, 29 2012 International Workshop on Information and Electronics Engineering 241–251 (2012.)

In the way cloud computing has been regulated till today, i.e. from the legal and regulatory approach, geographic location is of prime importance to enforcement[690]. Under the accountability regime, location becomes less relevant because of assurances that data will be treated as described regardless of jurisdiction[691]. Accountability can also contribute towards the enforceability of laws that apply to cloud computing either via the imposition of criminal penalties for misuse or with the assistance of technology[692].

Last but not least, the current regulatory structure places too much emphasis on recovering tools and procedures, if things go wrong, and not so much on trying to get cloud computing actors to 'do the right thing' for privacy in the first place[693]. On the contrary, a hybrid accountability mechanism built up via a combination of legal, regulatory and technological resources extending across public and private accountability domains is a practical way of securing effective cloud regulation[694]. Constructed in this manner, the accountability based regulatory framework for cloud computing can offer appropriate answers to the questions stemming from the privacy issues that arise and are rooted in cloud computing. In chapters 8 to 10 of this study, the legal principles of this accountability mechanism are described and analyzed.

690 Mark Gondree & Zachary N.J. Peterson (note 673).
691 Siani Pearson & Nick Wainwright (note 645).
692 Rolf H. Weber (note 677).
693 *Id.*
694 Siani Pearson & Nick Wainwright (note 645).