CHAPTER 10. Principles for regulating the cloud (3); the adoption of cloud computing regulation as the big leap forward from governing to governance in IT law

a. Introduction – scope of this chapter

Reference has already been made in earlier parts of this study[1089] to the need for cloud computing and the regulation of it to do the transition from a regime of governing to one of governance, more in touch with the real nature and features of the cloud phenomenon. In this chapter, following the analysis focusing on the technical and organizational/workflow aspects of the cloud, attention is paid to how this transition towards a new regulatory understanding regarding cloud computing can be set in motion and what are the fundamental concepts it should be based on. Moreover, concrete regulatory principles that will facilitate this transition are proposed for adoption by major jurisdictions with regard to the cloud phenomenon, again not with a view to homogenizing the way the cloud is legally dealt with but to making sure that, while respect will continue to be paid to the specificities and particularities of each jurisdiction and legal tradition, ultimately all major jurisdictions will work towards achieving comparable results/effects from the way cloud computing is regulated.

b. Doing laws based on the local and global experience: the differences in approach and the need to combine both perspectives in the case of cloud computing

State and all other regulators, of a lower or higher level, have to deal with an increasing number of policy matters that are defined by what is often described as a global, borderless nature. On the other hand, when called to produce laws that will be used for regulating these matters, those regulators have to work and formulate rules based on the experience and knowl-

1089 See Chapters 5 and 6.

edge they already have or to which they have access to and the objectives they wish to achieve through these regulations[1090], in terms of the results they hope to get back from applying these laws and the extent, geographic and material one, in which these laws will be applicable. This issue of being tasked with the production of laws applicable to a limited geographic area but having the potential to affect or touch upon issues that do affect the lives and activities of practically every law subject worldwide has been in the centre of attention of prominent scholars[1091], several of whom coming from the liberal movement. In particular, the tradeoff between regulating on the local and global level and the respective local or global knowledge upon which this rule making process is based has been at the centre of attention of Friedrich Hayek and his program[1092]. In Hayek's bipolar construction, on the one side lies 'the scope of the administrative state's regulatory jurisdiction; this is the large-scale question of government versus markets'[1093]. The second level is 'the internal organization of the regulatory bureaucracy, within the area committed to the administrative state's regulatory jurisdiction'[1094].

On each of the two sides of the equilibrium lie respective but substantially differing sources of knowledge, information, experience and expertise[1095]. In particular, on the one side there is the scope of the administrative state with its internal organization. On this side, Hayek puts emphasis on the benefits of local knowledge and adaptation to the contingencies of

---

1090 J. Goldring (note 258).

1091 This issue is continuously discussed in legal scholarship. For a thorough overview on it and its aspect which are of closer relation to this research, refer to: Martin Boodman, *The Myth of Harmonization of Laws*, 39 The American Journal of Comparative Law 699–724 (1991); Giandomenico Majone, *Policy Harmonization. Limits and Alternatives*, 16 Journal of Comparative Policy Analysis: Research and Practice 4–21 (2014); Antony Anghie & C.G Weeramantry, Legal visions of the 21st century: essays in honour of judge Christopher Weeramantry (op. 1998); M. J. Eger, *Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers*, 10 Law & Pol 1055–1105 (1978); Alfred Aman, *A Global Perspective on Current Regulatory Reform: Rejection, Relocation, or Reinvention?*, 2 2 Indiana Journal of Global Legal Studies 429 (1995) 429–464 (1995).

1092 Friedrich A. von Hayek, The road to serfdom (2005); Friedrich A. von Hayek (note 884).

1093 Friedrich A. von Hayek (note 1092).

1094 *Id.*

1095 Adrian Vermeule ed. (note 884).

time and place, but fails to do justice or downplays a major tradeoff: that centralized inclusive regulation is indispensable for epistemic coordination[1096]. As classic liberal theory teaches[1097], 'spillovers, externalities, and lost opportunities for economic synergy may arise not only because of conflicts of interest and problems of collective action, but also for epistemic reasons': in the chain of a production process for laws on the cloud, this translates into actors (i.e. legislators) with thick localized information who, confined by this short perspective, may be myopic about what other actors of the chain (i.e. the actors actively comprising the cloud computing workflow) are doing. In the end, a major challenge for any kind of law, no matter how extensive is the range of its geographical validity, is not just effective command-and-control, but also epistemic coordination and the creation of common knowledge and measures that 'dispel the local myopia of market actors'[1098].

In view of this double challenge for any kind of law, the question rises how all the relevant but also ample knowledge could be collected and coordinated in order to serve as the raw material for efficient, pragmatic and to-the-point laws. According to Hayek, the administrative state itself, with its range of institutions can take up the task of 'aggregating thick local knowledge, including the tacit, practical knowledge from daily experience'[1099] which is so crucial for the production of efficient legislation. Taking the case of the European Union as an example, the EU Parliament itself stands as a body of representatives with local knowledge from real life experience from different parts of Europe, while the various administrative agencies carrying some degree of competence on a given subject matter often incorporate actors with industry-specific or area-specific skills and information. The administrative state, which largely coincides with what we perceive as the (conventional) regulator, possesses much more than abstract or statistical technocratic expertise; every state structure, be it a national, federal or intergovernmental, even an international

1096 Michèle Lamont, *Rethinking Expertise. By Harry Collins and Robert Evans. Chicago. University of Chicago Press, 2007. Pp. 153. $37.50*, 115 American Journal of Sociology 569–571 (2009.)
1097 Adrian Vermeule ed. (note 884).
1098 *Id.*
1099 Friedrich A. von Hayek (note 1092).

one, has developed a representative bureaucracy devoted to the gathering and exploitation of local knowledge[1100].

In issues so complex as information technology and the cloud, there is heated debate as to which regulator is better qualified to do laws for them. There have been scholars who have argued in favor of local regulators and others who favor national or federal ones[1101]. As it has been argued throughout the course of this study, there is no right or wrong choice with regard to this issue. Actually, regulating the cloud is not an issue of who is better qualified to do it but rather of how it will be done and what it will aim for. In fact, actual state practice from national or federal states, proves that, absent some constitutional restrictions, regulatory bodies from all levels can intervene and regulate on most matters so that the subjects involved in each regulatory affair (for example, the actors that were presented in earlier parts of this study when it comes to cloud computing[1102]) can be constrained by state regulation as well as federal, in the case of federal states, or intergovernmental, as it happens, for instance, with EU law[1103]. Actually, provided that there is efficient coordination, in a number of domains federal or intergovernmental regulation may serve for clearing the way for state regulation that will ultimately contribute to regulatory uniformity, in order to reduce legal uncertainty.

In light of these, it must be made clear that the existence of multiple levels of regulators and regulations in no way undermines the importance of the administrative state's function to operate through command-and-control regulation[1104]. It is just that, in complex matters, such as the ones with which the law has to deal with in today's post-modern reality, this coordinating function[1105] of regulation may often be pursued through predominantly informational and epistemic measures[1106] instead of classic command-and-control rules.

Consequently, while the Hayekian construction succeeds in recognizing the two sides of actors when it comes to regulation prepared by the admin-

---

1100 Adrian Vermeule ed. (note 884).
1101 M. Gillen (note 415).
1102 See Chapter 9.
1103 *Id.*
1104 Adrian Vermeule ed. (note 884).
1105 Robert B. Ahdieh, *The Visible Hand: Coordination Functions of the Regulatory State*, 09 Emory University School of Law, Public Law and Legal Theory Research Paper Series 578–649 (2009.)
1106 *Id.*

istrative state, it stopped before realizing the importance of local knowledge towards efficient regulation, most likely due to the fact that complicated regulatory phenomena such as cloud computing were largely not a reality until a couple of decades ago. However, IT and cloud computing are perfect case studies to start off from Hayek's position and, after combining it with the principles of the theory on knowledge and the law[1107], to arrive in a modern formula that will guarantee the production of equally or, even better, more efficient regulation in the future.

Nevertheless, at the same time, Hayek's bipolar structure serves to conceptualize the competing pools of actors in the field of regulation and law making, in order for us to have the complete picture of dynamics that should be taken into account and need to be compromised in order for laws to actually work and achieve real results in the end. In particular, any law for a phenomenon so dynamic as the cloud cannot only aim at taming the forces of the market in favor of local knowledge about the needs that should be entertained from a particular set of rules. Actually, the market is only one of the institutional mechanisms for generating and then aggregating local knowledge[1108]. But it would be reckless to stress, from the one side, the importance of local knowledge for concluding efficient laws, and, at the same time, argue that only market mechanisms are good enough for collecting and aggregating it[1109]. Instead, one must carry out a fair institutional comparison between, or among, all institutional possibilities for contributing to the creation and maintenance of efficient laws. Specifically, and contrary to the voices putting forward the irrelevance of obsolescence of it, the regulatory state itself can still be justified as one of the key mechanisms for aggregating local knowledge. Similarly, as it has been repeatedly argued throughout this study, in the field of cloud computing regulation achieving the optimal results is not a question of choosing who, among competent potential regulators, does better or the best laws. Rather, what it is really needed is to coordinate among all these competent regula-

1107 I. Augsberg, Informationsverwaltungsrecht: Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen (2014.)

1108 D. Dyzenhaus & T. Poole, Law, Liberty and State: Oakeshott, Hayek and Schmitt on the Rule of Law (2015.)

1109 For additional considerations on the issue of how it is best to aggregate knowledge for regulating the cloud, refer also to the analysis on the theory of 'law and knowledge' and how it could be used as a valid method to construct a cloud regulatory framework as outlined in Chapter 7 of this study.

tors, to agree on elementary common principles that will define all the pieces of laws they may bring out and to make sure that, in the end, they will all work towards the same end result: a pragmatic and as timeless as possible regime of sound governance instead of an ever anxious to catch up with new standards regime of governing.

The next point of friction in the debate about how to build efficient laws for the cloud refers to the nature these laws should have, i.e. whether they should be designed with a broad and generic perspective in mind or whether they should be developed on an ad hoc basis, following actual developments within a regulator's area of competence the challenges and outstanding issues of which they would attempt to settle. In the theory of the administrative state as it has been promoted in the USA[1110], these two genres of law are described as synoptic and contextual laws, respectively[1111]. Although the terms are not unanimously adopted, they are the most illustrative ones in capturing the antithesis in thinking behind the style and philosophy of laws each of them represents. It also needs to be underlined that, of course, in reality there is no such clear-cut dividing line between the two types of laws; this dichotomy is more of a conventional scheme than a depiction of reality, in which there is expectedly a continuum between the two extremes[1112] and various degrees of synoptic or contextual elements in each piece of legislation. However, the scheme is useful in order for the possibilities that each path or type of law offers to be appreciated and comprehended.

If we would need to name one scholar as the leading proponent of synoptic laws, Justice Stephen Breyer of the US Supreme Court would probably be the most suitable choice. Throughout his scholarly path, Breyer has gone as far as expressing the idea that regulating risk via laws has become such a complicated challenge in modern societies that in effect it requires

---

1110 H. M. Collins, Tacit and explicit knowledge (2013.)

1111 Adrian Vermeule ed. (note 884).; D. Dyzenhaus & T. Poole (note 1108).. For further details on the antithesis between synoptic and contextual laws and the broader reasoning behind generic versus ad hoc approaches in scientific discourse, refer to: Ricardo Alonso, Wouter Dessein & Niko Matouschek, *When Does Coordination Require Centralization?*, 98 American Economic Review 145–179 (2008); Nicholas Bagley & Richard L. Revesz, *Centralized Oversight of the Regulatory State*, 106 Columbia Law Review 1260–1330 (2006).

1112 Stephen G. Breyer, Breaking the vicious circle. Toward effective risk regulation, vol. 1992 (1993.)

regulators who possess global knowledge[1113]. In his view, for any regulation to be a working one, 'it should achieve to reflect and take into account an overview of all socially or economically relevant risks for the subject matter it touches upon; it should attempt to present them in order of priority and it should regulate them just to the point at which the net social costs of regulation are equal to the benefits, but no more'[1114].

On the opposite side of synoptic regulation lies uncoordinated, socially wasteful regulation by a vast number of partially-informed and only to-a-certain-degree competent agencies and bodies. However, such a dispersed regulatory body is expected, and to an extent it has already been proved so, to suffer from three main drawbacks[1115]:

– tunnel vision[1116], a kind of obsessive focus in which regulatory agencies go as far as eliminating the entire amount of the particular risk within their jurisdiction, even if the costs of doing so far exceed the benefits;
– random agenda selection, which refers to the tendency of uncoordinated agencies to devote resources to regulating risks on different grounds than a ranking of expected social benefits; and
– Inconsistency, a condition in which uncoordinated agencies regulate similar risks differently or different risks similarly.

Such a picture could be observed overall currently with the myriad pieces of law regulating different aspects of cloud-facilitated IT applications and processes, due to the fact that there is still no common basis with regard to regulating their actual facilitator, i.e. the cloud. The problem occurs indeed not only within the same jurisdiction (i.e. in the case of federal states where both federal and regional or local bodies have concurrent competence) but also in the case of intergovernmental jurisdictions, such as the EU. As it has been observed, with the case of the American administrative state in mind: "decentralized organizations have a natural advantage in adapting decisions to local conditions, since the decisions are made by managers with the best information about those conditions. However, such organizations also have a natural disadvantage since the manager in charge of one division is uncertain about the decisions made by others."[1117]

1113 *Id.*
1114 *Id.*
1115 Michèle Lamont (note 1096).
1116 Adrian Vermeule ed. (note 884).
1117 *Id.*

However, as it has been explained, absolutely synoptic or contextual laws do not exist and all the more so, absolutely synoptically or contextually organized administrative structures do not exist either. Despite the assertions of both camps, neither can claim that they possess by privilege full rationality or absolute expertise; rather, bounded rationality affects both decentralized and centralized decision making[1118]. In a centralized orientation, bounded rationality manifests itself in a 'one size fits all' policy. In a decentralized arrangement, bounded rationality is traced as a lack of awareness of synergies across subdivisions. Instead, just as it was the case with the mechanisms for collecting and aggregating knowledge, law-making entities of all levels can be useful and have a role to play in efficiently regulating cloud computing. What is important in order for them to succeed in this aim is to coordinate among them so that they don't overlap with each other.

In summary, the distinction between local and global knowledge as well as the one between synoptic and contextual legislation is essential for understanding the issues of knowledge production, collection and aggregation as well as the topic of rule-making from all its aspects and extremes. As it has been demonstrated, the way regulatory bodies arrange how they collect and aggregate information as well as how they coordinate among themselves in order to define areas and subfields of competence ought to be a central agenda item in the debate and efforts for setting up a prescriptive and proactively oriented legal and political theory across a variety of topics and definitely with regard to cloud computing. Hayek's views, which served as the starting point for this discourse, may be directly relevant to these questions, but at the same time they have also turned out to be largely untenable. Regulation of complex issues such as the cloud cannot be left to just one type of actors relevant with the phenomenon, be them the market or regulators only. The market is definitely an important aggregator of information, including local knowledge but, at the same time, an imperfect one; on the other side of the administrative state construction lies another type of actors, equally essential but imperfect in themselves, i.e. all the different kinds of administrative authorities competent for the subject matter of a certain legislation, in our case all bodies that deal, one way or another, with cloud computing. All these entities do have and they will continue to have a meaningful role to play in the strive

1118 Stephen G. Breyer (note 1112).

to achieve efficient cloud regulation. Therefore, among the tasks of those that will be assigned to draft cloud computing laws should not be to try to prioritize the role and significance of certain bodies against others or, even more, to legislate that only certain among them are competent but some others are not. Instead, the task of a future body of cloud computing laws should be to coordinate the activities and regulatory priorities of all concurrent governing authorities of the field so that, in the end and while showing respect to the legal traditions and particularities of the environment within which each of them rules, the desirable effects of advanced legal certainty, coherence and market safety will be achieved for the cloud domain on an as universal level as possible.

c. The ability of law to learn and evolve; how to achieve law evolution in the case of cloud computing

Legal theory suggests in multiple ways that one of the cornerstone features of laws is their dynamic nature[1119]; their capability to change and evolve following respective social and political influences. As human societies progress or, anyway, develop economically, technologically and culturally, new challenges and disputes come to surface. As a rule, lower courts and other types of law applying bodies (e.g. arbitrators or independent authorities) decide on cases in light of existing legal rules[1120]; however, the results they achieve and the quality of the solutions proposed with their decisions eventually do not live up to changing political, social and cultural realities. It is precisely that moment when legislatures, rule-making agencies or higher courts are called to respond by modifying the legal rules or applying them differently, making sure that the results of their decisions will conform to the new realities[1121].

It is generally accepted that there are two ways in which the effect of a rule can be modified, specifically by

---

1119 John A. Ferejohn & Barry R. Weingast, *A positive theory of statutory interpretation*, 12 International Review of Law and Economics 263–279 (1992.)

1120 John T. Noonan (note 665).. For more scholarly analysis on the ways in which the effect of a rule can be modified as well as a succinct reply to L. A. Hart's approach refer to: Lon L. Fuller, *Positivism and Fidelity to Law. A Reply to Professor Hart*, 71 Harvard Law Review 630–672 (1958).

1121 John T. Noonan (note 665).

– changing the rule itself, for example, by making amendments to preconditions or modifying listed exceptions to the rule, or
– changing the meaning of the rule's constituent concepts[1122].

Most scholars refer to the first type of change as 'change in the rule's structure' and to the second type as 'change in the meaning of the rule's terms'[1123]. Change in legal rules and their concepts are essential elements for achieving the much-cherished dynamism of law, a feature that is becoming more and more crucial in today's continuously changing world[1124].

Nevertheless, despite the indispensability of change for both legal concepts and rules, the way in which each of the two progress and are modified is not identical. For starters, change in neither of them can be one-sided; it is rather organized in a manner that legal philosophers standardly call 'open textured'[1125], as it is not defined by necessary and sufficient conditions which are universally valid over their domain of application. Instead, according to Herbert Hart's theory of law, "legal concepts have a 'core of settled meaning' in which there is little debate over interpretation and a 'penumbra' in which interpretation is debatable. Legal rules derive their dynamic nature in part through the dynamic, open-textured nature of the terms used in the rules"[1126]. Of course, evolution does not affect only on the level of drafting (i.e. with regard to how regulators deal with them) but also on the level of interpretation of their meaning. Consequently, not only do "rules change when new prerequisites, exceptions, or conclusions arise, but also when new interpretations of terms used in the rule are made as cases are decided and rules are applied"[1127].

In light of the above, it becomes evident that in the field of cloud computing, as in many other fields, improving regulation is not only a matter of replacing existing laws with newer ones because older rules have been found to have become obsolete. Laws and overall legal certainty are also improved by putting in place basic regulation that will help us interpret and apply pre-existing legislation in a more coherent and in touch with

1122 *Id.*
1123 Robert B. Ahdieh (note 1105).
1124 Stephen G. Breyer (note 1112).
1125 Tomasz Zurek & Michał Araszkiewicz, Modeling teleological interpretation (2013.)
1126 H. L. A. Hart (note 664).
1127 John T. Noonan (note 665).

technological reality manner. In addition, improvement is also achieved by agreeing on the fundamental concepts and principles that should be at the core of all executive laws across different jurisdictions in order for law subjects to enjoy, as much as possible, comparable levels of protection with reference to an issue which is of a genuinely borderless nature.

The process of legislators and bodies applying the law is often paralleled to a learning system[1128]. In the end, it becomes clear that rules and their constituent terms change in light of the experience of deciding new cases or dealing with novel phenomena (when on the law-making level). However, there are fundamental differences in how legislatures, agencies and courts can effect, through their practice, this change in legal rules. Legislating bodies and agencies are the actors in a position to effect structural changes to laws[1129]. Courts process and evolve rules and definitions, too, thus they also effect structural changes, but beyond that, a court also has the capacity to change the meaning of a rule's constituent terms as it applies the rule in deciding a new problem[1130]. In several parts of this study we have seen several legal procedures before courts which have pointed out the need for IT laws to evolve and update themselves in view of developments in actual life and technology. Such occurrences of court decisions on cloud-related matters which point to a need for further refinement of cloud computing regulation have also existed in recent years[1131], further strengthening the call for adoption of shared fundamental principles on cloud computing regulation that will facilitate the transition from a regime of governing the cloud within each and every jurisdiction to one of cloud governance on a cross-jurisdictional and as geographically broad as possible basis.

These arguments regarding learning as an integral part of the process of law evolution and reform would not be complete without a few observations with regard to the inherent differences between a law learning process and one of some other discipline, such as physics or chemistry or of a

---

1128 Kevin D. Ashley & Edwina L. Rissland, *Law, learning and representation*, 150 Artificial Intelligence 17–58 (2003.)

1129 KIIT University ed., 2015 International Conference on Computational Intelligence & Networks (CINE.)

1130 *Id.*

1131 Namely, C-362/14 Maximillian Schrems v Data Protection Commissioner (note 417) as well as Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12 (note 486).

machine learning program[1132]. In fact, a law learning process is different from a machine learning program in the sense that the latter may discover a new law of physics, for example, out of instances of its application but does not and cannot create one. On the contrary, a learning process in the context of a law's application is not only limited to observing facts with a view to discovering the rules that explain them but it can also make use of the knowledge gained through these observations in order to create laws that will determine how the instances under observation could evolve. And actually, this evolution does not need to be identical to what has been observed so far; it can rather be essentially different.

While this observation could be the starting point of a philosophical discourse of considerable depth regarding how laws are evolving through and because of everyday practice and the knowledge accumulated out of it[1133], it does not suffice to explain the complex constraints on courts, and even on legislatures, in formulating and adjusting legal rules[1134]. Lawmakers are by definition and at an always accelerated pace challenged with accommodating developing ethical norms, economic and political principles, social policies, public expectations, past commitments and decisions, language-related conventions, and technological advances[1135]. These processes[1136] of discovering legal rules, subjecting them to rigorous scrutiny with regard to the above complex criteria, and evaluating the tradeoffs they effect can differentiate from one jurisdiction to the other and this is absolutely expected if differing legal traditions are taken into account. However, in essence, formulating legal rules is a process of discovering what will work in accommodating these criteria, not creating arbitrary norms out of nothing without consequences. Therefore, depending on the legal sector that is each time under focus, rule-making cannot be a laboratory process, 'sterilized' of any kind of influence from neighboring or generally important legal orders, let alone when their subject matter extends well

1132 International Workshop on Computational Autonomy (2003.)

1133 I. Augsberg (note 1107).

1134 Robert B. Ahdieh (note 1105).

1135 Kevin D. Ashley & Edwina L. Rissland (note 1128).

1136 For more extensive analysis on the types of process of law making and amendment, refer to: Edward H. Levi & Frederick F. Schauer, An introduction to legal reasoning (2013); Ronald Dworkin, Law's empire (1986); Cass R. Sunstein, *ON ANALOGICAL REASONING*, 106 Harvard Law Review 741–791 (1993); Scott Brewer, *Exemplary Reasoning. Semantics, Pragmatics, and the Rational Force of Legal Argument by Analogy*, 109 Harvard Law Review 923–1028 (1996.)

across the conventional margins among various jurisdictions. This interdependence is becoming all the more decisive in dynamic topics such as cloud computing. Insisting that the body of laws governing the cloud in one jurisdiction can be totally sealed against the expectations of its subjects falling under the competence of different legal orders but being potentially affected by the said body of rules as well, directly or indirectly, does more harm than good. Most importantly, it degrades the quality of the overall learning system through which constant law modification and update is possible. In the end, if IT laws are to remain relevant and improve their livability in view of the lightning speed at which the phenomena they address are changing, they need to prioritize towards a governance regime that will conserve legal cohesion in an as broader as possible area of application. And cloud computing regulation, as the body of rules that will govern the foundations of IT, is the ideal starting point for this change in perspective to be set in motion.

d. How proportionality and teleological reasoning can help cloud computing regulation make IT laws overall more efficient

Teleological reasoning is one of the oldest and most established norms in law making and interpretation[1137]. Proportionality is a relatively newer concept yet it has gained considerable relevance particularly in light of the ever more complex phenomena calling for regulation across conventional jurisdictional borders[1138]. These two norms combined can make an actual difference in both legislation and adjudication in the field of cloud com-

1137 Teleological reasoning is a term used by multiple disciplines to refer to a whole system of thinking which attempts to describe things in terms of their apparent purpose, directive principle, or goal. Its name stems from the word 'teleology' (from Greek telos, meaning end or purpose). For more details with regard to how teleology has been applied in law, refer to: Donald H. Berman & Carole D. Hafner, Representing teleological structure in case-based legal reasoning: the missing link (1993). For further insights into the teleological interpretation of laws refer to: Aharon Barak & Sari Bashi, Purposive Interpretation in Law (2011); Frank B. Cross, Theory and practice of statutory interpretation (2012.)

1138 Proportionality is a general principle in law which spans several special (although related) concepts. The concept of proportionality is used as a criterion of fairness and justice in statutory interpretation processes, especially in constitutional law, as a logical method intended to assist in discerning the correct balance between the restriction imposed by a corrective measure and the severity of

puting. The reasoning behind such an argument stems from the very essence of legislative action and the forces driving it. In details, according to an established argumentation of which Giovani Sartor is a champion, "legislative action can be guided not only by constitutional action-norms, but also by constitutional goal-norms, which are meant to govern the legislator's teleological reasoning (indicating what values should be ad-

---

the nature of the prohibited act. Within criminal law, it is used to convey the idea that the punishment of an offender should fit the crime. Under international humanitarian law governing the legal use of force in an armed conflict, proportionality and distinction are important factors in assessing military necessity. The proportionality test was first developed in the High State Administrative Courts (Oberlandesgericht) in Germany in the late 19th century, and was applied to review actions by the police. The concept has been greatly enriched within European Union law, in which there are generally four stages to a proportionality test, namely,
there must be a legitimate aim for a measure
the measure must be suitable to achieve the aim (potentially with a requirement of evidence to show it will have that effect)
the measure must be necessary to achieve the aim, that there cannot be any less onerous way of doing it
the measure must be reasonable, considering the competing interests of different groups at hand.
Definition derived from: https://en.wikipedia.org/wiki/Proportionality_(law) (lastly accessed on 11/29/2016).
For more background information on the concept of proportionality, refer to: P. P. Craig & G. de Búrca (note 287)..
Most recently, proportionality is a key consideration in the discovery process, and has been extensively applicable to the wider area of e-discovery, where it has been attributed with significant cost-savings. Already, it is considered that proportionality will be of particular significance to new and developing areas of law, such as the law of legal technology. With regard to this point, read more at: Klaus Schmidt & Alejandro Laje, *The Proportionality and Solidarity Principles and Their Impact on Privacy Laws in German Jurisprudence*, 5 Laws 27–38 (2016).
For further details on the concept of proportionality as fundamental principle of law, refer to: Tor-Inge Harbo, *The Function of the Proportionality Principle in EU Law*, 16 European Law Journal 158–185 (2010); Robert Alexy, *On the Structure of Legal Principles*, 13 Ratio Juris 294–304 (2000); Evelyn Ellis, The principle of proportionality in the laws of Europe (1999); E. Thomas Sullivan & Richard S. Frase, Proportionality principles in American law. Controlling excessive government actions (2009); Dieter Grimm, *Proportionality in Canadian and German Constitutional Jurisprudence*, 57 University of Toronto Law Journal 383–397 (2007).

vanced), rather than to limit the range of its admissible outcomes"[1139]. Adjusting this thesis in the field of IT law, one could claim that IT legislation and particularly any that focuses on fundamental elements of telecommunication technologies such as the proposed cloud computing regulatory principles, should not only care about settling unresolved issues at any given time that they arise but it should be constructed with the ultimate broader status quo that is hoped to be achieved in the field through it in mind. In addition, right-norms are increasingly proving to be of equal function as goal-norms with regard to legislators and public authorities[1140]. This is increasingly so in the IT sector, where, as it has been already demonstrated in earlier parts of this study[1141], there is increasing pressure on legislators on behalf of the public to modify existing or conceptualize new IT laws taking into account not just the need for fluent functioning of the market but also for upholding the general public's calls for better privacy, safety and security in their use of IT technologies.

As a result, any legislative review, especially if it refers to areas of law in which the rights of law subjects are so closely dependent with reference to their protection to the goals prioritized by legislators, must assess, design and implement any legislative and administrative action by "evaluating the proportionality (the teleological appropriateness) of legislative choices"[1142]. To this end, legislators nowadays and those that will deal with cloud computing regulation, in particular, should be directed in their work by the notion of reasonableness, an idea wishing to promote mutual institutional deference with the aim of ultimately achieving collaboration without overlapping: general legal theory suggests that "a margin of empirical and axiological appreciation should be left to legislators, even when constitutional values are at issue"[1143]. Similarly, cloud computing regulators need to work towards rules governing the cloud that will not only focus on settling the issues arising out of each particular application of cloud technologies only but rather they will aim to be of a long-lasting

---

1139 Giovanni Sartor, *Doing justice to rights and values: teleological reasoning and proportionality*. *Artificial Intelligence and Law*, 18 Artif Intell Law 175–215 (2010.)

1140 *Id.*

1141 See Chapter 3.

1142 *Id.*. For more on this notion refer to: Elen Stokes (note 888).

1143 Trevor Bench-Capon & Giovanni Sartor (note 956).. For more refer also to: Giorgio Bongiovanni, Giovanni Sartor & Chiara Valentini eds., Reasonableness and Law, vol. 86 (2009.)

and generic nature, as much as possible, so that the further-reaching goals of legal security and coherence of protection for all types of law subjects within the broader IT sector are achieved. This proposal for drafting cloud computing laws with a teleological mindset, if put forward across jurisdictions, helps us to further elaborate on the nature of cloud computing laws, which need to be inspired by a spirit of proportionality as well so that frictions and collisions among legal orders are softened as much as possible. Useful experience from other fields of law where cross-jurisdictional alignment has already been achieved to a substantial degree (for instance, from the field of trade law or the law of the sea) can also assist this process of integrating the teleological and proportionality methods deep into cloud computing law-making. Last but not least, given that the cloud terrain still is at this moment only loosely and case-based regulated, it is a unique opportunity to work on cloud regulation inspired by the teleological reasoning right from the beginning facilitating the establishment of a regime of governance over one of jurisdictionally fragmented governing in the sector.

e. How technology itself can help establishing a sound system of governance in the field of cloud computing

The idea of utilizing technology in order to protect data against the risks posed to them by technology itself has been discussed for years and it actually forms part of the whole cloud computing technological mindset[1144]: the cloud was put forward as a successor to previous technologies for handling data processes, among others, thanks to the fact that it left a lot of room for both technology gimmicks that would optimize data processing as well as others that would enhance the safety and security standards under which this would be conducted. Of course, the whole idea of making use of technology's powers against its malice has been put forward with varied tension and it has even reached the extreme of arguing that, "if threats to and violations of data protection are factually impossible, then there is no need to impose legal restrictions"[1145]. Needless to say, there is no need to choose between extremes; the alternative to too much regu-

1144 David S. Wall (note 661).
1145 Gerrit Hornung (note 735).

lation does not need to be no regulation at all. However, technology can indeed be a great asset in an effort to move from traditional restrictions encompassing obligations and prohibitions to a new regulatory approach focusing on proactivity and due diligence without the need for a breach that calls for punishment or repair, as it is currently the case. In fact, as Roßnagel put it back in 2001, "by adopting and executing normative requirements as to the use of personal data, law and technology complement each other and form an 'alliance' to protect personal rights"[1146], privacy and integrity of IT technology and cloud computing as a whole.

Collaboration between law and technology on the front of privacy, security and integrity of communications online is becoming increasingly important as traditional regulatory instruments are often unable to cope with the challenges of modern data processing[1147]. Many of those long-established IT rules, being tied to the conventional enforcement authorities of national states, lose a considerable amount of their effectiveness in the fluid social sphere of the internet[1148]. Under these circumstances, effective data protection in today's cloud-dominated IT landscape cannot be guaranteed by legal instruments alone. Instead, a mixture of up-to-date, proactively oriented and precautionary regulations along with suitable technological assets and the series of specialized laws already in place is the key to achieving the best possible level of integrity, safety and security in the vast amount of cloud-facilitated applications. As data processing becomes pervasive, privacy enhancing technologies are increasingly important and an indispensable tool in the effort towards establishing a sound system of governance with regard to cloud computing and the entire environment of applications around it. Actually, the idea that technological support is indispensable in sealing data against the risks they face from technology-assisted processing is so strongly supported that in certain areas of comput-

1146 Alexander Rossnagel, Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz; Dokumentation der Stiftungstagung (zugleich EMR-Workshop), der Alcatel SEL Stiftung für Kommunikationsforschung, des Instituts für Medienrecht (EMR), der Landeszentrale für politische Bildung (LpB) Baden-Württemberg, am 10. Mai 2001 im Landtag Baden-Württemberg, Stuttgart, Bd. 24 (2001.)

1147 R. K. Lippert & K. Walby, *Governing Through Privacy*. *Authoritarian Liberalism, Law, and Privacy Knowledge*, 12 Law, Culture and the Humanities 329–352 (2016.)

1148 M. Friedewald & R. J. Pohoryles (note 119).; Alexander Rossnagel (note 1146).

ing it appears as a sine qua non. Specifically, in ubiquitous computing[1149], it appears[1150] to be "a misperception to believe that it is possible to secure personal privacy and informational self-determination without technologies that provide anonymity, pseudonymization and transparency in a user-controlled way without hampering the user in his or her everyday business"[1151]. Such technologies are already available and they could not only be used in reinforcing generic cloud computing laws of the nature and scope that have been analyzed in the previous chapters, but they could also make possible privacy-friendly settings in cloud-based systems and appli-

1149 Ubiquitous computing (or "ubicomp") is a concept in software engineering and computer science where computing is made to appear anytime and everywhere. In contrast to desktop computing, ubiquitous computing can be exercised using any device, in any location, and in any format. A user interacts with the computer, which can be in many different forms, including laptop computers, tablets and terminals in everyday objects such as a fridge or a pair of glasses. The underlying technologies supporting ubiquitous computing include Internet, advanced middleware, operating system, mobile code, sensors, microprocessors, new I/O and user interfaces, networks, mobile protocols, location and positioning and new materials. (https://en.wikipedia.org/wiki/Ubiquitous_computing; lastly accessed on 11/29/2016)
Ubiquitous computing is also described as pervasive computing, ambient intelligence, or "everyware". Each term emphasizes slightly different aspects. Several experts suggest that an evolution of the concept of ubiquitous computing is also the notion of Internet of Things, when primarily concerning the objects involved. Ubiquitous computing touches on a wide range of research topics, including distributed computing, mobile computing, location computing, mobile networking, context-aware computing, sensor networks, human-computer interaction, and artificial intelligence. For more information on ubiquitous computing, refer to: Eva Nieuwdorp, *The pervasive discourse*, 5 Comput. Entertain. 13 (2007); Adam Greenfield, Everyware. The dawning age of ubiquitous computing (2006); Stefan Poslad, Ubiquitous computing. Smart devices, environments and interactions (2009).

1150 Giovanni Sartor (note 1139).; For additional information refer also to: Elgar Fleisch & Friedemann Mattern, Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis : Visionen, Technologien, Anwendungen, Handlungsanleitungen (2005); Alexander Roßnagel, Tom Sommerlatte & Udo Winand, Digitale Visionen. Zur Gestaltung allgegenwärtiger Informationstechnologien (2008.)

1151 Gerrit Hornung (note 735).. In addition with reference to this point, read: Alexander Roßnagel, Datenschutz in einem informatisierten Alltag (2007); Mireille Hildebrandt, *Profiling and the rule of law*, 1 IDIS 55–70 (2008).

cations, facilitate the much promoted opt-in principle[1152], make possible the configuration of personalized user-settings for routine data processing, speed up and optimize automatic deleting processes, permit the deployment of personalized identity management or transmit systems, organize, aggregate and document declarations of consent that any data subject may have issued for certain types of data processes etc.

Moreover, it should not be overlooked that, if the precautionary perspective is supposed to be the one with most relevance to a governance regime with a character as generic as possible in the field of cloud computing, technology-based sealing and protective measures are an invaluable supplement to cloud computing regulation. Besides, it should not be forgotten that arranging a precaution-oriented regulatory landscape with regard to the cloud will, in the future, be increasingly relevant since the growing amount of data processed via cloud networks, in the form of big data collected amass via IoT systems, respectively increases the risk that huge amounts of data subjects become identifiable, even though until recently such identification was not possible[1153].

Last but not least, it must be stressed out that any concept for data protection and technology-assisted cloud computing regulation needs to be designed by having two target groups in mind: producers of the respective technologies, as they were analyzed above[1154], who need to be legally obliged to ensure actual availability of the said technology, and users, that is, the various actors within the cloud workflow as they have been previously analyzed[1155], with the aim of forcing them to actually put these measures in practice. Both target groups need to have clear guidelines from regulators for the development and application of privacy-friendly tech-

---

1152 The opt-in principle in privacy law is a concept appearing in several jurisdictions and pieces of laws regulating aspects of privacy and refers to the active and affirmative consent of user and data subject to submit itself to the terms and conditions under which the data-involving processing at hand takes place. For more on the principle and its essence, refer to: Siani Pearson (note 728); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 Stan. L. Rev. Online 63–69 (2011); Eve M. Caudill & Patrick E. Murphy, *Consumer Online Privacy*. *Legal and Ethical Issues*, 19 Journal of Public Policy & Marketing 7–19 (2000); Alfred Kobsa, *Privacy-enhanced personalization*, 50 Commun. ACM 24–33 (2007.)

1153 Alexander Roßnagel (note 1151).

1154 See Chapters 8 and 9.

1155 See Chapters 8 and 9.

nologies. At the same time, making official the adoption of such technologies, as an indispensable asset towards the establishment of the new governance-oriented regime in the field of cloud computing, will encourage actors of these groups to actually invest resources and effort in developing and implementing such technologies. It is up to regulators' bravery to make the body of cloud computing laws as relevant as possible at this point, by going as far as concretizing future-oriented criteria for the design of technology that may be even directly derived from cloud computing regulation[1156]. What is more, cloud computing laws could even provide business and growth opportunities or even incentivize the use of such technologies.

In conclusion, it should be pointed out that, much as the cloud has been a liberalizing force for IT markets per se, market forces alone are not a sufficient force for the development and spreading of PETs and, in general, technological applications aimed at enhancing the integrity of cloud networks. There are several reasons for this and, as usually with everything regarding the cloud, economies of scale are a primary one. In other words, technology is as a rule designed with a view to responding to certain functional requirements. Contrary to what the average non-technically mind may think, enhancing privacy is not, from a technical point of view, a functional requirement in itself[1157]. The most important (and legitimate, as we are talking about actors of an economic activity) aim of actors throughout the cloud workflow is the maximization of profit. In view of that, optimum data protection, the integrity and maximum coherence of the network are as relevant as demand of the network's offerings on the market continues to exist. If this demand is lowered, this may quickly become a counterforce for the technology tweaks discussed here, which could end up being irrelevant in the design process because they may either increase or they may not reduce costs. Therefore, much as cloud regulation could be benefited from technology assets in its effort to make the passing from a regime of case-based governing to generically established governance, it should not take this collaboration between law and IT for granted; rather, it should take positive action and institutionalize it.

1156 Alexander Roßnagel, Tom Sommerlatte & Udo Winand (note 1150).

1157 Gerrit Hornung (note 735).; Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 Yale Law Journal 868–890 (2009.)

f. The key to achieving a sound system of governance in cloud computing regulation: legal interoperability and its significance as a concept in transnational law

Interoperability is a fundamental element of the entire IT sector and cloud computing, in particular. Today's IT networks are so highly interconnected among them that there are devices which are not built at all to function properly on their own, but must interact with other elements of software or hardware[1158]. Actually, by today's IT standards, it is even possible that a device that cannot interoperate with other products with which consumers expect it to do so to be considered essentially worthless[1159].

Maintaining the position which has been at the core of this study from the beginning, that regulating the cloud is a fundamentally interdisciplinary issue, it is now time to see not only how law should adapt to technological standards in order to efficiently govern cloud computing but also how and if legislation could profit from technological state-of-the-art. With this approach in mind, it is proposed that the concept of interoperability should extend beyond its purely technical dimension and make an important contribution to the development of transnational IT law, in general, and cloud computing regulation per se. Departing from the technological context of interoperability, there have been scholars who have brought forward the concept of cultural interoperability[1160]; this idea is now time to be further transplanted in the legal discipline, in which there have been already some voices championing for legal interoperability, in the sector of IT law, in particular. Legal interoperability should be, in other words, one of the core elements in the nature of laws that will be designed for governing the cloud.

Looking to define what legal interoperability constitutes of one needs to go back to the original concept of technical interoperability. Although no universal or unequivocally accepted definition of technological interoper-

1158 KIIT University ed. (note 1129).

1159 Ian Watson, The universal machine. From the dawn of computing to digital consciousness (2012.)

1160 Amedeo Santosuosso & Alessandra Malerba, *Legal Interoperability as a Comprehensive Concept in Transnational Law*, 6 Law, Inn Tech 51–73 (2014.)

ability really exists, two distinct components have been largely recognized[1161]:

– syntactic interoperability, which refers to the ability of diverse systems to communicate with each other and exchange data;
– semantic interoperability, which denotes the ability to interpret and use those data and pieces of information in a significant way, useful to the end user.

Mutatis mutandis, in the field of IT law interoperability is as efficient as each of these two elements are entertained, which means that:

– syntactics become all the more coherent as the legal discipline learns to communicate better with other sciences and exchange know-how and knowledge with them;
– semantics improve as the legal discipline learns to interpret and use the knowledge and know-how it receives from other sciences in such a way that they can help it with its goal to produce better rules, more suitable for the actual challenges of the IT reality.

In the context of technology, there are several ways in which syntactics or semantics can be improved, both technical and legal ones. For instance, intellectual property (IP) licensing agreements (as an example of a legal tool) and the use of open standards (as an example of a technical tool) are just two of the various methods in which the above components can be intensified and become more apparent[1162]. Following this logic, legal interoperability in the context of cloud computing regulation does not need and should not be a one-direction process, i.e. the legal sector only learning from the technical one. Much as legal rules need to be adapted to the technological status quo of the cloud, once put into force, if they have been designed taking into account how technology is and where it is heading at the time of their inception, can also point the way of technological advancement by broadening the route for aspects of this advancement that are believed by tech experts to be beneficial for the industry and end users or setting limits to other types of future progress which are feared to have a potentially derailing or adversary effect.

Nonetheless, interoperability does not receive a carte blanche in its technical and nor should it be given unlimited freedom in its legal dimension. As much as it is true that IT systems interoperability is an essential

1161 eHealth Governance Initiative, DISCUSSION PAPER ON SEMANTIC AND TECHNICAL INTEROPERABILITY (2012.)

1162 Amedeo Santosuosso & Alessandra Malerba (note 1160).

step forward, and there are numerous advantages (such as innovation, competition, flexibility and openness) which have been greatly boosted thanks to it[1163], there are many drawbacks that have been pointed out as well. In fact, IT scholars have expressed their concerns in relation to issues of security and privacy, as well as about the risk of excessive homogeneity[1164] or the so-called 'lock-in problem'[1165]. These are only a few indicators that revolutionary or groundbreaking as technical interoperability may be, it cannot be left to go unabated and without limits. Similarly, legal interoperability should not be adopted unconditionally nor should it be left to function beyond control in the cloud computing law making process and any other IT law making process for that matter. As it has been argued before, the legal discipline should maintain the upper hand and this can be not only protective for the final degree of efficiency of cloud computing laws, it can even be beneficial to the pace at which these laws will gain in efficiency overall.

Far-fetched as it may seem, the idea of legal interoperability is not an unrealistic one and the field of cloud computing regulation may actually be one of the most suitable sectors for this concept to be put into practice first. As a matter of fact, the conception of law as technology, which has been already analyzed in the course of this study[1166], can serve as a feasible frame for legal interoperability. That is to say, if it taken for granted that "political power or jurists can (as the theory of law as technology does) easily handle law, it should also be true that they could make law interoperable (if they wanted it)"[1167]. It goes without saying that the question is more complex and extends far beyond the aims of this study. However, as it will be argued in the conclusions of this analysis, one of the benefits of legislators actually settling down to deal with the challenge of cloud computing regulation can be that this so unique task will actually constitute a first and bold step towards bringing to the center of attention

1163 John G. Palfrey & Urs Gasser, Interop. The promise and perils of highly interconnected systems (2012.)
1164 *Id.*
1165 John G. Palfrey & Urs Gasser (note 235).
1166 See Chapters 4, 5 and 8.
1167 Amedeo Santosuosso & Alessandra Malerba (note 1160).

not only the need for horizontal but also for vertical interoperability[1168]. As to why IT and cloud computing law, in particular, could be an ideal starting point for putting interoperability at the heart of the rule making process, for now it is enough to recall the teachings of Carl Schmitt who was one of the first legal theorists that expressed the view that "law in modernity is another technology"[1169].

Last but not least, interoperability should of course not be interpreted only in relation to other disciplines or sectors of law but it should also have an interjurisdictional meaning. Having in mind the current status quo with regard to jurisdiction in cloud computing issues and the questions that the current regime leaves unanswered, as these were analyzed earlier[1170], interjurisdictional interoperability in cloud computing regulation should be constructed with the aim of explaining and encompassing the following aspects:

- answer why currently the way the cloud is regulated is neither unified nor uniform, in space and time (fragmentation) and what it needs to be done to achieve at least minimum working uniformity without pushing for unrealistic (and unnecessary) unification.
- answer why relevant IT laws are currently not hierarchically organized in a coherent way and how cloud computing regulation could contribute to that direction.
- it should always save room for flexibility for itself and not develop in a necessarily directional manner, as a crucial role in the field of IT and the cloud will always be played by spontaneous developments, be them unforeseen technological advancements or applications of current technologies which do not fit any of the known technical models till that time.
- it should develop taking into account all the different actors taking part in the wider cloud computing cycle, either as integral actors of the

1168 The issue of vertical vs. horizontal interoperability of laws, in particular IT ones, is a vast one and extends beyond the scope of this analysis. However, for a brief introduction to the issue, refer to: Xenofon Kontargyris, From effective to efficient regulation of ICT (2): the big leap towards embracing vertical, apart from horizontal, interdisciplinarity, available at: http://www.juwiss.de/88-2016/ (13 September 2017) (lastly accessed on: 09/13/2017.)

1169 Jens Meierhenrich, Oliver Simons & Friedrich Balke, The Oxford Handbook of Carl Schmitt, vol. 1 (2015.)

1170 See Chapter 5.

cloud workflow[1171] or on a cross-border basis[1172]. The differences of them in nature and legitimacy need to be reflected in the wording and spirit of cloud computing laws.
– interjuridictionally oriented cloud computing laws need to be processed always having in mind that they will continuously form part of a highly technified global environment.

g. A brief summary of the trends on privacy regulation through time in a global context; the transit to a cloud computing regulation governance regime is not a free fall into the unknown

From the beginning and across several parts of this analysis we have extensively talked about the various regulatory approaches on privacy and which of them managed to surface as the prevailing ones in major jurisdictions through time. Although emphasis was mostly given to the most recent concepts of privacy, i.e. the ones that were influenced or even initiated by the arrival and gradual establishment of IT, the idea of privacy in relation to different types of communication among people has been on the table since much longer and there are several exemplary references to that in previous parts of this study. It is beyond the scope of this project to make a detailed history review of the concept of privacy; yet, given that it is the one idea that had dominated regulatory and policy-making thinking with regard to IT technologies for a long time and, despite the fact that it may have lately been partially overshadowed by newer concepts of security or consent, it still remains among the pillars of IT regulation, it is worth summarizing the main trends about it. One more reason for doing so is that it will help us realize that the transition or, more precisely, the introduction of the proposed governance regime for cloud computing technologies alongside the rest of specific laws already in place for particular applications of them is no free fall from the sky; rather regulators and scholars have already suggested elements of the proposed regime in their discourse so far, just in a scattered manner. What needs to be done now is for competent regulatory and law-making bodies to gather all these ideas which are dispersed throughout literature and policy debate, bring them together, supplement them with the original perspectives that have been pre-

1171 See Chapter 9.
1172 See Chapter 6.

sented in previous chapters of this analysis and build up the much-needed fundamental common governance principles on cloud computing regulation.

To begin with, the four prevailing ways of defining privacy over the years since the concept was introduced as one of the main challenges with regard to any kind of interpersonal communication are[1173]:

- the non-interference concept[1174]
- the limited accessibility concept[1175]
- the privacy as information control concept[1176]
- a fourth concept incorporating various elements of the other three proposals but limiting the applicability of the idea of privacy to intimate or sensitive aspects of people's lives.

Each of these generic conceptions of privacy has found more or less welcoming ground across various jurisdictions and has served as the raw material for building the respective sets of laws on privacy regulation. It goes without saying that there was a varying degree in which each of these concepts had remained pure or undergone adaptations to reflect on each jurisdiction's views and long-held values on the issues relevant laws were set to settle each time. Out of all major jurisdictions and the main manifestations of them through time, there have been of course specific instances which stand out for their effectiveness, their outreach as well as their progressiveness. Among them, the German data privacy regime is often cited by many as one of the most successful[1177]. Although by the standards of a considerable number of scholars it is thought to be too rigid, one can hardly deny that the German privacy regulatory apparatus has traditionally featured a comprehensive, well-founded legislative platform with a solid constitutional footing and several progressive features, such as a legal requirement that organizations appoint internal privacy officers[1178]. Another of these elements exemplary of how German legal discourse has treated the notion of IT privacy with a clearly forward-thinking nature at certain mo-

1173 L. A. Bygrave (note 137).
1174 It is regarded by many as the oldest conceptualization of privacy. Originally, it was suggested in: Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, IV Harvard Law Review 193–220 (1890.)
1175 A reference text for this concept of privacy is the following: Ruth Gavison, *Privacy and the Limits of Law*, 89 The Yale Law Journal 421–471 (1980.)
1176 L. A. Bygrave (note 137).
1177 Ulrich Dammann & Spiros Simitis (note 169).
1178 Anne Arendt, Ulrich Dammann & Spiros Simitis (note 742).

ments (although it did not prevail in the end) is the principle of 'systemic data protection' ('Systemdatenschutzprinzip')[1179]. Brought on the table as early as the beginning of the 1990s, this notion suggested the integration of data privacy concerns already in the design and development of information systems architecture, a line of thinking which surprisingly fits very well with many of the modern challenges posed by cloud computing technologies. Needless to say, promoters of that principle did not have in mind the cloud-based IT landscape we are faced with nowadays; even so, it is very interesting and useful to see that a regulatory framework such as the one described here would not be an unfounded or reckless move from a legislative point of view, just as it is no such one from a technical perspective. Regulatory thinking has already demonstrated remarkable forwardness and open-mindedness and it is not at all beyond its capacity to take the big leap and introduce a set of regulatory principles of common understanding such as the ones proposed in this study. Of course, what will make the big difference this time and what constitutes a substantial originality compared to the past is that the proposed cloud computing governance framework is based on a proactive and precautionary approach rather than on a corrective or remedial one.

h. Making a long-lasting governance regime a choice not a necessity

To sum things up, there have been numerous different approaches on privacy, security and other neighboring concepts that have been cited throughout this extensive analysis which has been attempting to discern

---

1179 For an analytical overview on the Systemdatenschutzprinzip and the ways it has lately been discussed or suggested that it could be utilized in the context of the German data protection regime, refer to: Martin Rost, *Standardisierte Datenschutzmodellierung*, 36 Datenschutz Datensich 433–438 (2012); Marit Hansen, *Datenschutz nach dem Summer of Snowden*, 38 Datenschutz Datensich 439–444 (2014); Volker Lüdemann, Alfred Scheerhorn, Christin Sengstacken & Daniel Brettschneider, *Systemdatenschutz im Smart Grid*, 39 Datenschutz Datensich 93–97 (2015); Steffen Kroschwald, Informationelle Selbstbestimmung in der Cloud. Datenschutzrechtliche Bewertung und Gestaltung des Cloud Computing aus dem Blickwinkel des Mittelstands (2016); S. Jandt, S. Kroschwald, A. Roßnagel & M. Wicker, *Datenschutzkonformes Cloud-Computing*, in Cloud-Services aus der Geschäftsperspektive, 207–266 (Helmut Krcmar, Jan Marco Leimeister, Alexander Roßnagel & Ali Sunyaev eds., 2016.)

among the whole lot and bring together only the ones crucial or relevant to cloud computing. There may be equally many others less relevant to the focus point of this project but still totally important approaches to different aspects of IT regulation. A significant number of them are also clearly progressive, inspired by liberal teachings in the fields of philosophy, human rights, economics or other fields. And all these progressive approaches together make a clear point towards the direction of a liberal governmentality[1180].

There have already been indications that particular regulatory bodies are beginning to realize the importance of regulating IT technologies not with a view to correcting any harm done as quickly as possible but with the aim of preventing it from happening as efficiently as it gets[1181]. One could say that on the regulatory front which focuses on how cloud networks should be designed things are already half a step ahead[1182], with the notion of 'privacy by design' quickly gaining ground. In this context, "privacy is to be thought-through ahead of time, that is, 'designed', 'set', 'planned'."[1183] It involves techniques and technologies that fashion privacy in new forms and 'packaging' and they even come up with ways to commercialize the various levels of it, beyond the basic one, as commodities[1184]. As its supporters champion, privacy by design may apply to "IT systems, accountable business practices, and physical design and networked infrastructure,"[1185] bringing to surface its remarkably wide and growing scope.

This is almost certainly the most advanced and forward-thinking specimen of IT-related regulatory approach that has been conceptualized so far. Yet, for the time being, it is limited on the technical design aspect of the

1180 Kristina Irion (note 220).
1181 Jean-Christophe Graz & Andreas Nölke, Transnational private governance and its limits, vol. 51 (2008.)
1182 Elen Stokes (note 888).
1183 R. K. Lippert & K. Walby (note 1147).
1184 Peter Hustinx, *Privacy by design*. *Delivering the promises*, 3 IDIS 253–255 (2010); A. Cavoukian, Privacy by Design; The 7 Foundational Principles, available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
1185 R. K. Lippert & K. Walby (note 1147).

whole matter[1186]. The time is now to benefit from this future-oriented thinking that is gradually gaining strength on the technology or technical regulation front and expand its spirit to the entire spectrum of cloud computing regulation[1187]. Agreeing or researching and bringing together the best of what EU or US law and practice has to offer with regard to handling specific aspects of the cloud phenomenon and fortifying all these with the decisive yet clearly science- and fact-based ideas that have been analyzed on the course of this analysis will not be some reckless act but rather a strategic step ahead. Most importantly, it will give a decisive push towards the direction of cultivating a long-lasting, coherent and generic governance regime that it can come up with answers to many more challenges than the already existing ones which will be a choice and not necessity.

i. Can the transatlantic divide on privacy be bridged? Why the extensive use of cloud computing technologies makes the call for convergence an urgent one?

Having extensively analyzed the issue of cloud computing regulation with a particular focus on privacy regulation in the cloud from the perspectives of EU and US law, we have already reached the conclusion that better regulation on these issues does not necessarily mean that one law (or legal culture) should succumb to the other. Instead, it is more of a process whereby the two jurisdictions will agree on common goals or shared weaknesses and venture on seeking ways in which they could pursue the former or tackle the latter.

For starters, it can be argued without reservation that differences between the two systems of laws are often overstated, while mutual interests, especially on the part of law subjects and the civil society of are overlooked. As a matter of fact, none of the two regimes in its present form is perfect: EU law still provides ground for intrusions on privacy in the name of national security, and thus may be less protective than it is often as-

1186 For an indicative example of how old the observation of greater technical in comparison to legal advancement in the field of IT is refer to: Aron Mefford, *Lex Informatica: Foundations of Law on the Internet*, 5 Indiana Journal of Global Legal Studies 211–237 (1997.)

1187 M. Gillen (note 415).; David S. Wall (note 661).

sumed. At the same time, existing legal safeguards in the US are clearly insufficient in light of the revealed technological capacities of agencies such as the NSA over the last years, yet those revelations have prompted all three branches of government in the States to reassess NSA practices and relevant regulations in place, while they have also mobilized civil society[1188]. And as anxiety about privacy increases in the US, concerns about national security have dramatically risen in Europe following the series of terrorist attacks in several European cities over the last years. At the end of the day, the EU and the US may well be converging more than diverging with respect to national security surveillance and the great majority of measures taken in that front typically involve surveillance of data and communications largely hosted and facilitated by cloud computing.

Nobody denies that thanks to the relevant body of EU law, the CJEU has developed extensive case law in the field of privacy and data protection, establishing itself and the European Union as the leading jurisdiction in the field[1189]. However, at the same time, the EU data protection regime features a number of weaknesses and derogations which dilute its overall capacity to protect privacy rights[1190]. For starters, the EU data protection framework permits member states to restrict the rights granted to data subjects in the Data Protection Regulation for broad reasons of national security, defense or public security[1191]. This is a natural consequence of the division of competences between the EU and member states: the EU has only restricted authority to legislate in the field of security, and has already adopted a considerable range of measures coordinating law enforcement activities of the member states, or establishing EU counter-terrorism and security policies[1192]. However, under Article 4.2 TEU, "national security

1188 See also Chapter 3.
1189 See also Chapter 3 and 4.
1190 David Cole & Federico Fabbrini (note 32).
1191 Such reasons as grounds for restricting the applicability of the General Data Protection Regulation are to be found in several provisions of the GDPR, most notably in: cl. 16 pream. and Art. 23 Regulation (EU) 2016/679 (GDPR) (note 25).
1192 V. Mitsilegas, European union and internal security. Guardian of the people? (2014); Tridimas, T., & Gutierrez-Fons, J. A. (note 217); Alexander Roßnagel, *Datenschutzfragen des Cloud Computing*, in Wolken über dem Rechtsstaat? Recht und Technik des Cloud Computing in Verwaltung und Wirtschaft, 19–52 (Alexander Roßnagel ed., 2015.)

remains the sole responsibility of each Member State."[1193] As a result, this contradiction creates potential room for undermining of the overall protections granted by the Regulation which cannot be so easily quantified a priori given that the measures which may put it in question could as well stem from national and not European law. What is more, although there are minimum common rules for personal privacy established in the ECHR[1194], Europe's other major text regulating fundamental rights and freedoms besides the body of EU law, national rules demonstrate significant variations, with certain states providing advanced protection for privacy, while others lag behind. The GDPR aspires to cure this imbalance, yet the loopholes it potentially leaves for national legislators to divert from its core provisions still allow suspicion as to whether the status quo of privacy will be unanimous throughout the Union to flourish[1195].

Second, European data protection law is unlikely to place any serious obstacles to surveillance operations of EU member states conducted outside the EU (including infrastructure facilities, such as storage installations empowering cloud services). In accordance with the principle of loyal cooperation enshrined in Article 4(3) EU Treaty[1196], EU law sets limits to the actions of the EU member states' intelligence agencies in other EU member states[1197]. On the contrary though, it remains silent on member states' surveillance outside the EU[1198]. The picture does not get any clearer by the ECHR either, as neither that set of rules imposes significant limits on surveillance outside a member state's borders.

1193 The Treaty on European Union (TEU), C 115/13, 2008.

1194 Federico Fabbrini, Fundamental rights in Europe (2014.)

1195 On the broader issue of room for national derogations to the rules of the GDPR, see W. Gregory Voss, *Looking at European Union Data Protection Law Reform Through a Different Prism. The Proposed EU General Data Protection Regulation Two Years Later*, 17 Journal of Internet Law 1–3 (2014); Rothenberg, M., Jacobs, D., *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 Harv. J. L. & Pub. Pol 606–652 (2013); V. Chang, Delivery and Adoption of Cloud Computing Services in Contemporary Organizations (2015); S. Meachem, *Cloud With a Chance of Regulation*, 57 ITNOW 18–21 (2015); Alexander Roßnagel ed. (note 285).

1196 "Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties."; The Treaty on European Union (TEU), C 115/13, 2008.

1197 David Cole & Federico Fabbrini (note 32).

1198 David Cole & Federico Fabbrini (note 32); V. Mitsilegas (note 1192).

Equal obscurity remains on the European Court of Human Rights (ECtHR) front. Europe's top court for fundamental rights violations has repeatedly interpreted Article 8 ECHR, which grants a right to private and family life, as incorporating a right to data protection[1199] as well. Nevertheless, the ECtHR has never directly dealt with the case of surveillance operations exercised outside Europe and against foreign persons[1200]. Consequently, the ECtHR has yet to extend any Article 8 ECHR protection to a foreign national outside the jurisdiction or control of a contracting state.

In conclusion, while the EU Charter of Fundamental Rights and the EU data protection legislation undoubtedly establish a comprehensive framework to safeguard privacy in the era of digital communications and the cloud, states still have discretion with respect to national security surveillance[1201]. Consequently, while strong protections are in place within the geographical margins of EU law as well as in many cases with considerable elements of externality, neither EU law nor the ECHR for the time being seem to be able to constrain EU member states' surveillance of foreign nationals beyond their borders. This grey zone though leaves enough room for undermining people's privacy rights, especially when it comes to operations targeting data which are being handled via cloud computing, where the link for determining jurisdiction always stands on thin air, as we already discussed[1202].

Turning to the US, one has to admit that US law does not have any kind of systematized body of rules remotely resembling the General Data Protection Regulation, while existing constitutional precedents tend to give the government a relatively free reign with respect to data collection, particularly when it is done in the context of surveillance operations such as the NSA programs. But on further reflection, differences between the US and the EU may not be as stark as commonly thought. Especially when one focuses on the issue of surveillance activities.

Following US constitutional law, the US government has since long formulated two doctrines as legal basis for the constitutionality of its agencies' surveillance activities. The first stipulates that the Fourth Amend-

1199 L. A. Bygrave (note 137).
1200 David Cole & Federico Fabbrini (note 32).
1201 Maria Tzanou, *The EU as an emerging 'Surveillance Society'. The function creep case study and challenges to privacy and data protection*, 4 ICL Journal (2010.)
1202 See also Chapter 6.

ment does not protect information that individuals share with "third parties."[1203] As a result, the Fourth Amendment does not prevent the US government or any of its agents from obtaining such information, as long as they do so from the third party with whom the individual has shared such details.

Second, US courts have ruled that at least in certain cases the Fourth Amendment does not govern US officials' search of a foreign national's home abroad[1204]. This ruling, academic analysis finds, also includes search and seizure operations aimed at digital data of foreigners which are maintained on facilities away from US jurisdiction[1205].

To sum up, US law recognizes and protects privacy, both as a constitutional, Fourth Amendment matter, and as a statutory matter.[1206] For the most part, though US privacy laws are most protective when the government seeks to collect information within the US, about US citizens or permanent residents, nothing is explicitly stipulated with reference to digital surveillance operations aiming foreign nationals abroad; the only exception to this rule is certain discussions which have been provoked by concerns that such surveillance might intercept communications of foreign nationals where US citizens were also involved.

In light of the analysis above as well as in several other parts of this study, it seems that the issue of efficient protection and regulation of privacy and cloud computing is not suitable for proclaiming outright winners or losers between EU and US law; on the contrary, both legal systems have their strong and weak points, while they both leave considerable room for uncertainty when it comes to the protection of data of subjects which are foreign to their jurisdiction and the instance affecting their data takes place outside their geographic area of competence as well.

There are a number of very strong policy arguments why data protection and overall cloud regulation should be better coordinated between Europe and America. It is beyond the scope of this study to consider political, defense or military reasons why better coordination in regulating the

---

1203 See also Chapter 3.

1204 David Cole & Federico Fabbrini (note 32).; see in particular: United States v. Verdugo-Urquidez, 494 U.S. 259, 259 (1990.)

1205 Christopher Slobogin, Privacy at risk. The new government surveillance and the Fourth Amendment (2007); Orin Kerr (note 231).

1206 See also Chapter 3.

cloud is desirable[1207]. But it needs to be pointed out that there are also strong economic interests for both the EU and the US to support a transatlantic coordination in the field of cloud computing regulation. The US and the EU are the biggest trading partners in the world[1208]. At the same time, the rise of digital economy creates powerful incentives for them to enhance interconnectivity between their markets as well as between the laws that deal with any issues they might arise. The field of cloud computing regulation is probably the fundamental regulatory discipline where this coordination should begin from.

1207 For extensive analysis on these reasons that make better coordination between EU and US on the issue of cloud regulation refer to: David Cole & Federico Fabbrini (note 32); Johannes Thimm, Inseparable, but not equal. Assessing U.S.-EU relations in the wake of the NSA surveillance affair, 4/2014 (2014.)

1208 Refer also to Chapter 3.