CHAPTER 11. Conclusion

a. The driving forces that make the need for cloud computing regulation a pressing one

Throughout this analysis, it has been stressed out that cloud computing, as a pioneering way of taking advantage of the best data processing technologies have to offer, calls for a fresh look into the regulatory tools governing the wider IT phenomenon. These new regulatory frameworks do not need to be viewed as a substitute for current laws but rather as their natural but urgent successor, an original take on the IT governance starting from the cloud phenomenon as the core element of information technology and dealing with it from a broad, generic perspective, thus laying the general legal principles upon which any specialized IT legislation could be safely and with continuity developed in the future.

There may well be critical voices of this idea, i.e. the need for a regulatory framework focusing on the cloud as the foundation of information technologies and communication; yet, numbers and data from both the computer and legal science fronts suggest otherwise. In fact, latest numerical data suggest that the range and abundance of uses of cloud computing are growing at an exponential rate over the years, fueled recently by the push given to data industry by big data-related applications. Actually, analysis of the types and diversity of big-data centered uses of cloud computing indicates that technology is evolving so fast that is it driving the cloud's evolution at a pace much faster than any regulatory attempt from the existing ones could possibly effectively tame[1209].

1209 Chaowei Yang, Qunying Huang, Zhenlong Li, Kai Liu & Fei Hu, *Big Data and cloud computing. Innovation opportunities and challenges*, 10 International Journal of Digital Earth 13–53 (2016); Divyakant Agrawal, Philip Bernstein, Elisa Bertino, Susan Davidson, Umeshwas Dayal, Michael Franklin, Johannes Gehrke, Laura Haas, Alon Halevy, Jiawei Han, H. V. Jagadish, Alexandros Labrinidis, Sam Madden, Yannis Papakonstantinou, Jignesh Patel, Raghu Ramakrishnan, Kenneth Ross, Cyrus Shahabi, Dan Suciu, Shiv Vaithyanathan & Jennifer Widom, *Challenges and Opportunities with Big Data 2011-1* Cyber Center Technical Reports (2011); Divyakant Agrawal, Sudipto Das & Amr El Abbadi, *Big data and cloud computing. Current state and future opportunities* 530–533

At the same time, statistical analysis on the research done so far on cloud computing and extensive literature review on available resources on the broad topic reveal that the legal aspects of the cloud phenomenon remain largely unexplored. This is not so much because there is not considerable output on the legal and ethical challenges posed by the cloud already but rather because many of its technical feasibilities remain at a nascent level but tend to gain attention and develop at lightning speed once they gain the research communities attention. In particular, according to content analysis conducted for 236 scholarly journal articles published between 2009 and 2014 with the aims of

– Identifying possible trends and changes in cloud computing over the six years of the survey,
– comparing publishing productivity of journals about the cloud computing subject, and
– guiding future research about cloud computing

the results of which were published in 2016, the majority of cloud computing research output is about "cloud computing adoption" (19%), followed by the "legal and ethical issues" of cloud computing (15%). However, at the same time it was observed that numerous technical aspects of the cloud, which had remained mostly unexplored until recently are picking up pace really fast once they attract researchers' and industry's attention. For example, technical issues such as "cloud computing for mobile applications" and the "energy consumption dimension of cloud computing", which were found to be among the least explored and researched topic areas at the beginning of the study, started growing at a remarkable pace once they became hot topics for the cloud industry and relevant to the existing or upcoming cloud-based applications[1210]. (4%) are the least attention grabbing themes in the literature. However, "cloud computing for

(2011); Mauro Andreolini, Michele Colajanni, Marcello Pietri & Stefania Tosi, *Adaptive, scalable and reliable monitoring of big data on clouds*, 79-80 Journal of Parallel and Distributed Computing 67–79 (2015); Marcos D. Assunção, Rodrigo N. Calheiros, Silvia Bianchi, Marco A.S. Netto & Rajkumar Buyya, *Big Data computing and clouds*. *Trends and future directions*, 79-80 Journal of Parallel and Distributed Computing 3–15 (2015.)

1210 Merve Bayramusta & V. Aslihan Nasir, *A fad or future of IT? A comprehensive literature review on the cloud computing research*, 36 International Journal of Information Management 635–644 (2016). For further information regarding the vast research questions and opportunities around the cloud which still remain unexploited, refer also to: Marc Fouquet, Heiko Niedermayer & Georg

mobile applications" and "energy consumption dimension of cloud computing" themes have become popular in the last two years, so they are expected to be trendy topics of the near future. Another important finding was that the majority of the articles indexed during the study were published by engineering, information systems or technical journals such as "IT Professional Magazine", "International Journal of Information Management" and "Mobile Networks and Applications" which means that legal aspects of the cloud have until largely been collateral points of research focused on cloud computing and there is still ample room for dedicated legal analysis on cloud computing[1211].

At the same time, technical research into more advanced ways to monitor cloud environments is evolving at full speed paving already the way for applications and tools that can be deployed to track activity or optimize use of cloud networks in ways totally novel to what is known for the time being and what has been taken into account by regulators when writing existing laws for cloud-enabled applications[1212].

Carle, *Cloud computing for the masses*, in Proceedings of the 1st ACM workshop on User-provided networking challenges and opportunities, 31 (Paulo Mendes ed., 2009); Rekha Saluja, *Cloud Computing: Challenges and New Developments*, 5 International Journal of Science, Engineering and Computer Technology 173–176 (2015); Nabil Sultan, *Cloud computing. A democratizing force?*, 33 International Journal of Information Management 810–815 (2013); Mladen A. Vouk, *Cloud Computing – Issues, Research and Implementations*, 16 CIT 235–246 (2008.)

1211 Merve Bayramusta & V. Aslihan Nasir (note 1210). For further details on the multiple research aspects posed by cloud computing and its widespread use actors sectors of economy refer to: Gerald Münzl, Michael Pauly & Martin Reti eds., Cloud Computing als neue Herausforderung für Management und IT (2015.)

1212 Guilherme Da Cunha Rodrigues, Rodrigo N. Calheiros, Vinicius Tavares Guimaraes, Glederson Lessa dos Santos, Márcio Barbosa de Carvalho, Lisandro Zambenedetti Granville, Liane Margarida Rockenbach Tarouco & Rajkumar Buyya, *Monitoring of cloud computing environments*, in Proceedings of the 31st Annual ACM Symposium on Applied Computing, 378–383 (Sascha Ossowski ed., 2016). For additional resources on the future trends in technical tools for monitoring and managing cloud resources and networks, refer also to: Georgios Tselentis, Towards the future internet. Emerging trends from European research (2010); Jesús Montes, Alberto Sánchez, Bunjamin Memishi, María S. Pérez & Gabriel Antoniu, *GMonE. A complete approach to cloud monitoring*, 29 Future Generation Computer Systems 2026–2040 (2013.)

For all these reasons, it is firmly believed that the systematic analysis and collection under the same project of best practices, current trends and proposals for a sound cloud computing regulation that was attempted throughout the course of this study is an important one and could serve as the starting point for regulators to put together in the near future much more sound and better coordinated rules for the cloud-enabled IT landscape of today and tomorrow.

b. Overview of solutions and suggestions towards the development of sound cloud computing regulation regimes

The following is a summary of the proposals made throughout this study towards achieving cloud computing regulatory frameworks that will be more in line with the speed and frequency in which IT is evolving nowadays and will also provide for greater certainty for legal subjects on a cross-jurisdictional basis. It should be reiterated that the outcomes of this analysis are based on the preconditions set for it already in its introductory chapter. Moreover, given that the project is essentially a comparative analysis between norms and trends of two jurisdictions aiming not in proclaiming winners and losers but rather in bringing together best practices from and for both of them, some of the following propositions may not struck readers coming from one of the two schools of legal thought (i.e. the EU and US one) as absolutely original or ground-breaking. Yet it needs to be born in mind that this work has been meant as a synthesizing effort between the two jurisdictions it focuses on and, consequently, ideas which may be standard practice in one jurisdiction can be essentially new approaches for the other and vice versa.

The summary of the proposals made over previous chapters of this analysis is structured under three categories, i.e. normative, governance and policy ones.

i. Normative proposals

As normative are coined proposals which stem from theory of law and, ultimately, push towards the direction of cloud computing rules that will not be understood simply as an additional set of laws for IT but rather as a set of fundamental principles that will serve as the foundation of IT law:

– Currently, it is not uncommon that technological advancement may bypass regulatory prudence in the time between the initialization the conceptualization phase for a law and the time it is concluded causing a vicious circle. An exit from this pattern can only be achieved if cloud computing regulation deviates from the norm currently followed by IT laws that are largely ad-hoc formulated and takes a more technologically abstract yet intra-jurisdictionally systematic direction. In other words, cloud computing regulation should not serve as a cure to technological implementations that may go wrong but should change its focus on making sure that the margin for accidents from cloud-enabled technological applications (presently known or even forthcoming ones) is limited to the biggest extent possible[1213].
– Cloud regulation laws should refrain from undue restrictions. Experience and history indicate that in dynamic phenomena, such as cloud computing, restrictive approaches usually either hinder progress or are simply rendered invalid via a workaround. Consequently, it does not seem meaningful to try to control what will happen next in a sector by forbidding certain things from happening. The key to better regulation is definitely not greater or unjustified restrictions[1214].
– The legislators' mindset should be towards fostering a predictable, minimalist, consistent and simple legal environment. In fact, many scholars agree that this should not be just the wish pursued with every new adopted legislation but rather the primary goal future laws should serve: ensuring that the regulated environment in which law subjects will be let to act will be a simple-to-understand and opaque one[1215].
– Given the prevailing legal doctrine regarding IT technologies and the data tasks effectuated through them, the essential elements of an effective regulatory regime for the cloud should be transparency, availability and accountability. Transparency is an important element in the struggle to meet security, privacy or trust obligations, since it brings to the forefront the (contractual) will of all cloud actors (be them users, service providers, inspecting authorities etc.) to fulfil the globally accepted privacy principles that will make up for a sound and secure cloud environment. Availability arises as a prerequisite since in a sound governance framework for the cloud availability for reporting and inspec-

1213 For more refer to Chapter 4.
1214 For more refer to Chapter 5.
1215 *Id.* See also Chapter 4.

tion of cloud actors is of prime importance as an assurance for application of the commonly accepted privacy and security requirements. Finally, accountability is an important factor arising directly from one of the main legal challenges with regard to cloud computing: namely that commitments from parties to the cloud life cycle must be clear and enforceable in practice. This, in consequence, stimulates trust throughout the cloud cycle and further intensifies the bonds between providers and users of cloud services[1216].

– Laws for the cloud, primarily those focusing on determining competent jurisdiction, should be developed in the future having the theory of reasonableness in mind. This, according to Lowenfeld suggests that any set of rules 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"[1217]. This concept is intended to help resolve particular situations, typical among which are those when there is a jurisdictional conflict between regulators in two sovereign states[1218].
– Regulators tasked with developing laws for the cloud should work bearing the external and internal perspective of every IT phenomenon about to be regulated in mind. According to them, 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. When it comes to plain users, there can be those who have an understanding of both realities simultaneously; technically savvy users, with a certain 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

1216 For more refer to Chapter 7.
1217 Dan Svantesson (note 548).
1218 For more refer to Chapter 6.

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 it to provide thorough and not partial answers[1219].

– There are lots of different ways to deploy the same kind of infrastructure and this means that the (regulatory) challenges coming with one type of cloud environment will not necessarily be the same with those of another. For instance, a great deal of issues regarding privacy raised by public clouds are non-existent or they are satisfactorily tackled when the same resources are utilized to set up a private cloud computing network. However, the technical expertise, the mechanical skills and the very materials (i.e. pieces of hardware) that are necessary in order to build up either a public (with just the standard protection features) or a private (with as advanced protection features as possible) cloud ecosystem are, in essence, the same. In both cases, and in every other in between, one will need pieces of the same kind of infrastructure, the same kind of information science and IT engineering knowledge that will permit one to put those pieces of hardware into meaningful working arrangements and, of course, even the features that will differentiate them and make them stand apart from each other will be based on the same technical principles and scientific intel that makes the overall concept of cloud computing technology possible. Consequently, it becomes evident that, despite the great variety in which cloud services and networks appear on the market and the substantial differences which might exist between all these variations of cloud environments, there is a common underlying connecting tissue that binds them all, and that is the knowledge (of informatics, computing engineering and other disciplines) related to them which is one and the same. With these in mind, the challenge is not to homogenize IT laws or pulverize jurisdictional particularities. It rather is to set common

1219 For more refer to Chapter 6.

goals and establish rules that will contribute to their achievement. The path towards achieving these goals can and will expectedly be different, both because cloud computing manifests itself through various different arrangements and because two or more identical cloud networks in different environments will naturally be treated in differentiated manners according to the legal culture in each environment. However, as long as the same purposes are pursued and, ultimately, materialize, the path and the means need not be identical[1220].

– Rules developed with the goal of regulating the cloud apart from putting emphasis on clearing out which cloud actor is tasked with what specific duties at each time throughout a cloud network's workflow, should also provide clear rules for shedding light on the issue of superiority between conflicting rules affecting the same areas of cloud-related activity putting an end to the insecurities that still so manifestly exist despite an already wide range of legal tools attempting to deal with all outstanding issues in the wider field of IT[1221].
– It is strongly recommended that a future regulatory framework for cloud computing should be based on a definition that will not only describe what cloud computing does, from a technical perspective, but also explain its dual nature as a concept, i.e. that it is not just about the external manifestations we see of it but also about the way the underlying technology and hardware are organized around certain actors to construct, all together, a dynamic and continuously changing business workflow. In this way, the subsequent rules will not only reflect on the external but also on the internal aspect of cloud computing dealing with the whole range of cloud-related issues calling for regulatory arrangement[1222].
– While laws on the applications made possible thanks to cloud computing technologies usually adopt a punitive or repressive approach trying to describe in what way harmful effects from malpractice with these applications could be limited, cloud computing regulation should adopt a primarily proactive approach focusing on who is charged with what functions and duties in that context throughout the cloud network. In this manner, it is expected that affected entities will be better aware of their duties and the preparations required to live up to depending on the

1220 For more refer to Chapter 8.
1221 For more refer to Chapter 9.
1222 Id.

role(s) they are playing within a cloud network, thus increasing the chances for smooth and transparent function of the cloud market and minimizing the odds for harmful events or spillovers thereof[1223].

– IT and cloud computing are perfect case studies to start off from Hayek's position on the regulatory state and, after combining it with the principles of the theory on knowledge and the law, to arrive in a modern formula that will guarantee the production of equally or, even better, more efficient regulation in the future. 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, 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 regulators, 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 product: 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[1224].
– In the field of cloud computing, as in many other fields, improving regulation is not only a matter of replacing existing laws with new 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 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[1225].
– 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

1223 Id. See also Chapter 4.
1224 For more refer to Chapter 10.
1225 Id.

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. Cloud computing regulation, as the body of rules that will govern the foundations of IT, is the ideal starting point for this new regulatory perspective to be set in motion[1226].

– 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 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[1227].
– Substantial integration of the spirit of the 'Systemdatenschutzprinzip' in future laws for the cloud. 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

1226 Id.
1227 Id.

with many of the modern challenges posed by cloud computing technologies[1228].

ii. Governance proposals

As governance proposals are coined those that do not explicitly need additional regulations but could already fit with existing IT laws; however, they imperatively must be taken into account when cloud computing laws are designed in the future:

– The GDPR invests a lot on a priori over a posteriori regulation, which is in principle of course better. Notwithstanding, it still interprets a priori protection as a range of procedures and checklists data controllers have to go through before any specific data processing and not as some clearly formulated, aim-oriented general principles which will make clear the level of protection that is to be maintained at all times during a data processing cycle irrespective of how this will be achieved by any given data controller. In other words, what we need for a data protection regime looking to the future is not more forms or compliance questionnaires; the real challenge is to let everyone know under what quality standards data are expected to be processed and let them then decide how to achieve them, knowing that, should they fail, equally clear repercussions will be faced[1229].
– Pre-cloud facilities were designed with a primary objective to get the data processing done in a clearly laid-out and secure manner. Cloud-based facilities are constructed with the primary aim of getting data processing done in an as user-friendly as possible manner and with a priority on optimizing economies of scale for the provider but also the user of the cloud infrastructure. This change of focus resulted in the security of the processing not being possible to be taken for granted anymore. From a status quo where it was enough to know what role each of the actors participating in a data processing sequence held in order to be able to identify their responsibilities and duties, we are today in a situation where the data processing workflow is geographically and resource-wise dynamic and spread-out across the cloud facility, hence

1228 Id.
1229 For more refer to Chapter 4.

calling for a different approach that will guarantee security and transparency throughout the processing workflow[1230].

– It is suggested that the cloud industry be reorganized based on an end to end accountability approach. 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 accountability will not be vague nor will it only be affirmed when a wrongdoing occurs. 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. 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[1231].
– 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 computing it appears as a sine qua non. Specifically, in ubiquitous computing, it appears to be "a misperception to believe that it is possible to secure personal privacy and informational self-determination without technologies that provide anonymity, pseudonymity and transparency in a user-controlled way without hampering the user in his or her everyday business". Such

1230 Id.
1231 For more refer to Chapter 6.

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 previous chapters, but they could also make possible privacy-friendly settings in cloud-based systems and applications, facilitate the much promoted opt-in principle, 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[1232].

iii. Policy proposals

The last set of recommendations includes policy proposals, i.e. specific measures that can be taken within each jurisdiction as well as on a cross-jurisdictional basis towards bringing the suggestions from two previous categories into effect:

– Future privacy laws should stipulate broad categories of uses and services involving data, certain of which will also be permissible without or with only limited, standardized safeguards. For riskier applications involving data, future regulatory schemes should articulate ground rules for how data users will determine the dangers of a particular data use or service and determine thereafter what measures best avoid or mitigate them[1233].
– 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

1232 For more refer to Chapter 10.
1233 For more refer to Chapter 4.

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[1234].

– 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. 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 constantly hold the different actors accountable for their share of duties in the broader task of making sure the cloud cycle runs smoothly[1235].
– The relationship between the two pools of laws, i.e. the already existing and abundant one of laws regulating cloud-based applications and the currently nascent or almost non-existent but needed one of rules regulating the cloud per se, should not be hierarchical but rather complimentary: enriching the latter should be done in a way that will further boost the efficiency of the former[1236].
– In every law-making process governments or, in general, legislative authorities, have a certain range of mechanisms available to detect legal and regulatory issues related to the subject matter of the laws they are about to design. As it is commonly admitted, what issues do finally make it onto the legal and regulatory agenda greatly depends on the prevailing political economy in which an issue, in this case cloud computing, emerges and diffuses; accordingly, these conditions may vary across countries. As far as the cloud is concerned, although the two jurisdictions under examination in this study (i.e. EU and the US) may be following distinctly separate routes in the way they handle IT and, in particular, data-related issues, in both of them there is a strong momentum in civil society for taking decisive measures and adopting laws that will clear out the current blurry picture when it comes to regulating cloud technologies. This unanimous call for action should be heard by regulators and, apart from being a call for them to act, it can also serve as a perfect tool in working on producing rules for the cloud that will be based on common principles and will, therefore, be possible to

1234 For more refer to Chapter 6.
1235 Id.
1236 For more refer to Chapter 9.

be presented to both jurisdictions with an increased likelihood of being met favorably and embraced by all affected actors[1237].

– 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, 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, 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 technologies. 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. What is more, cloud computing laws could even provide business and growth opportunities or even incentivize the use of such technologies[1238].

c. Future challenges – insights for further research

As it has been demonstrated, big data constitute the latest wave in the tsunami-like development of modern information technologies. Being a phenomenon which has been around only for a handful of years, they have grown exponentially and managed to play a decisive role in the final shaping and spirit of IT laws as new as the EU's GDPR. However, technological progress is relentless and, just as the world tries to process all the challenges big data have brought about, further waves of change are already looming on the horizon. The Internet of Things (IoT), the growth of which was, to a large extent, propelled by the success of big data, is quickly expanding in multiple directions beyond personal data. And just as the range

1237 Id.
1238 For more refer to Chapter 10.

of IoT applications multiplies so does its interrelation with the cloud[1239] and the challenges raised[1240]. For instance, soon it will become clear that it is not only important that the data collected on the cloud via IoT installations are safe and sealed from malpractice but that the metadata that will be produced as the output of processing activities carried out on the cloud are equally reliable, solid and accurate[1241]. Moreover, the proliferation of IoT applications and systems already challenges long-held legal perceptions in the field of IT, such as the illegality of hacking; there are already voices indicating that in the face of the diversity of IoT installations and the wide range of dangers that may be associated to them, even hacking should be considered a possibility under regulated circumstances[1242].

In conclusion, the issues dealt with on the course of this research are so dynamic that they could turn it into a never-ending project, should we wish to cover every single aspect and type of challenges cloud computing poses for IT law. Without being able, in the duration and with the constraints of a single PhD term, to provide answers to all questions, it is hoped that the points raised and the solutions proposed throughout this analysis will serve as a driving force for more pragmatic and more durable IT laws in the future, in an effort to maximize the benefits from the galloping advancement of technology for all types of actors, from users to service providers to regulators to the law itself and the security and sentiment of safety it should convey to its subjects.

1239 Everton Cavalcante, Jorge Pereira, Marcelo Pitanga Alves, Pedro Maia, Roniceli Moura, Thais Batista, Flavia C. Delicato & Paulo F. Pires, *On the interplay of Internet of Things and Cloud Computing. A systematic mapping study*, 89-90 Computer Communications 17–33 (2016.)

1240 Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko & David Eyers, *Twenty Security Considerations for Cloud-Supported Internet of Things*, 3 IEEE Internet Things J. 269–284 (2016); Christopher Rees, *Who owns our data?*, 30 Computer Law & Security Review 75–79 (2014); Niels Fallenbeck & Claudia Eckert (note 932); Birgit Vogel-Heuser, Thomas Bauernhansl & Michael ten Hompel eds., Handbuch Industrie 4.0 Bd.4 (2017.)

1241 For an example of beyond the norm cloud-based application which poses unprecedented regulatory challenges with regard to massive data exchanges and processing refer to: Fruzsina Molnár-Gábor & Jan O. Korbel, *Regulierung neuer Herausforderungen in den Naturwissenschaften – Datenschutz und Datenaustausch in der translationalen genetischen Forschung*, in Messen und Verstehen in der Wissenschaft. Interdisziplinäre Ansätze, 151–171 (Marcel Schweiker, Joachim Hass, Anna Novokhatko & Roxana Halbleib eds., 2017.)

1242 Ido Kilovaty, *Freedom to Hack* SSRN Journal (2017.)