CHAPTER 4. An introduction to the definition of cloud computing under EU law and the challenges it poses

a. Introduction – scope of this chapter

According to European Commission's White Paper on the cloud: "'Cloud computing' in simplified terms can be understood as the storing, processing and use of data on remotely located computers accessed over the internet. This means that users can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfil their needs and that they can get to their data from anywhere with an internet connection."[261]

Based on this definition, the Commission had recognized back in 2012 certain key areas where regulatory actions were needed: Fragmentation of the digital single market due to differing national legal frameworks and uncertainties over applicable law; digital content and data location, which ranked highest amongst the concerns of potential cloud computing adopters and providers; problems with contracts related to worries over data access and portability; change control and ownership of the data[262]. The current labyrinth of standards generates confusion by, on one hand, a proliferation of standards and on the other hand, a lack of certainty as to which standards provide adequate levels of interoperability of data formats to permit portability.

In its Digital Agenda for Europe[263], the Commission set itself the objectives to achieve the digital single market, enhance interoperability and standards, strengthen online trust and security, simplify copyright clearance, management and cross-border licensing, goals that have gained importance as a result of the prevalence of cloud computing as the standard technology in the field of data processing.

---

261 European Commission (note 242). (last accessed on: 01/18/2017.)
262 *Id.*
263 (note 241).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Adopting the definition of cloud computing which the US National Institute of Standards and Technology (NIST) released in its Special Publication SP 800-145 in September 2011[264], European Commission's Art. 29 Working Party brought out in 2012 a cornerstone document for the treatment of cloud computing in Europe, usually quoted as the 'Sopot Memorandum'[265]. In that paper, Art. 29 WP highlighted the most important issues that the cloud poses for European regulators, which include[266]:

- there is not yet an international agreement on common terminology;
- the development of the technology is still in progress making unclear the precise landscape that needs to be regulated;
- enormous amounts of data are being accumulated and concentrated posing even more challenges that stem from cloud technologies which facilitate these processes;
- cloud technology is boundless and transboundary;
- data processing has become genuinely global;
- transparency is lacking with respect to cloud service provider processes, procedures and practices, including whether or not cloud service providers sub-contract any of the processing and if so, what their respective processes, procedures and practices are;
- this lack of transparency makes it difficult to conduct a proper risk assessment;
- this lack of transparency also makes it more difficult to enforce rules regarding data protection;
- cloud service providers are under great pressure to quickly capitalize significant investment costs;
- cloud customers are under increasing pressure to reduce costs, including those of their data processing; and
- to keep low prices cloud service providers are more likely to offer standard terms and conditions.

264 Peter Mell & Timothy Grance (note 63).

265 International Working Group on Data Protection in Telecommunications, Working Paper on Cloud Computing – Privacy and data protection issues. "Sopot Memorandum", available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-3 (3 February 2015.)

266 *Id.*

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

In the same document, Art. 29 WP laid down the major risks associated to the surge of cloud computing[267]:

- breaches of information security such as breaches of confidentiality, integrity or availability of (personal) data that go unnoticed by the controller;
- data being transferred to jurisdictions that do not provide adequate data protection;
- acts in violation of laws and principles for privacy and data protection;
- the controller accepting standard terms and conditions that give the cloud service provider too much leeway, including the possibility that the cloud service provider may process data in a way that contradicts the controller's instructions;
- cloud service providers or their subcontractors using the controllers' data for their own purposes without the controllers' knowledge or permission;
- accountability and responsibility seemingly fading or disappearing in a chain of subcontractors;
- the controller losing control of the data and data processing;
- the controller or its trusted third party (e.g. auditor) being unable to properly monitor the cloud service provider;
- data protection authorities being precluded from properly supervising the processing of personal data by the controller and the cloud service provider; and
- the controller relying on unfounded trust in the absence of insight and monitoring, thereby potentially contravening the data protection legislation in force in the country of establishment.

In light of the above, the aim of this chapter is to present an overview of how cloud computing has been progressively defined under EU law as well as put together the most important critique and arguments regarding the efficiency of the Union's latest cornerstone regulation in the wider area of IT law, i.e. the General Data Protection Regulation. Finally, in the last sections of the chapter analysis will be focused on how a heavily cloud-based IT landscape looks like (or is expected to look like, in a few years' time). This analysis will then serve, along with findings from following chapters, to determine the rate at which existing IT laws applicable when it comes to cloud regulation have achieved the required level of maturity

267 *Id.*

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

and efficacy with regard to the subject matter they are supposed to settle and how they should evolve in the future.

b. The most important policy views on aspects of cloud computing brought out so far and why they are not yet sufficient

During the last decade, since the cloud started to rapidly gain ground as a data handling technology, actors in the EU and the US market with a direct or indirect interest in the relevant fields have formulated a number of policy manifestos that contain the main current views on the cloud and how it should be dealt with from a regulatory perspective. By summarizing the main principles of these views one can then more easily point out the loopholes in the way the cloud has been treated so far by regulators[268].

Purpose limitation used to be a key concept in the EU's data privacy legislation[269] during the DPD era, which largely served as the basis for any regulatory approach for cloud computing. In particular, purpose limitation protected data subjects[270] by setting limits on how controllers[271] were able to use their personal data[272]. The concept of purpose limitation was built on two main ideas: personal data had to be collected for 'speci-

268 Article 29 Working Party, Opinion 03/2013 on purpose limitation, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (3 February 2015.)

269 Hunton Privacy Blog, Article 29 Working Party Clarifies Purpose Limitation Principle; Opines on Big and Open Data, available at: https://www.huntonprivacyblog.com/2013/04/09/article-29-working-party-clarifies-purpose-limitation-principle-opines-on-big-and-open-data/ (5 November 2015.)

270 By 'data subject' in the context of IT and privacy law reference is made to an individual entity who is the subject of personal data.

271 A 'controller' is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". Definition as it appears in Regulation (EU) 2016/679 (GDPR) (note 25).

272 'Personal data' is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Definition as it appears in Regulation (EU) 2016/679 (GDPR) (note 25).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

fied, explicit and legitimate'[273] purposes (purpose specification) and could not be 'further processed in a way incompatible'[274] with those purposes (compatible use). It should be noted that further processing for a different purpose does not necessarily mean that there is a breach of the purpose limitation: compatibility is assessed on a case-by-case basis.

This Art. 29 WP Opinion was meant to apply to all kinds of data transfers, i.e. also to those effected through the use of cloud computing technologies. Given that, so far, European regulators tend to approach the task of regulating the cloud through the prism of already existing legislation for specific uses of it, such as data transfers, several elements of the practical application of the purpose limitation principle lead to a need for an in-depth analysis of this concept, which, after all, decisively defined EU data protection law:

– The way privacy limitation has been implemented in Member States has led to a diversity of interpretations over it[275]. If we are to keep applying it in data transfer related legislations in the future, a clear common understanding of the concept will better ensure its effective application – and that would be, of course, in the interest of all concerned.
– The context of processing activities needs also to be updated and amended to reflect today's standards[276]. The development of new technologies, such as cloud computing, results in increasingly more data being available, for a far wider diversity of purposes.
– Apart from the traditional concept of data transfer, i.e. transferring data between two points of a linear or at least insulated network, there are many more current trends for reuse of data by the private sector ('big data') but also 'open data' and 'data sharing' initiatives proposed by many governments, including EU legislative initiatives[277]. These practices which have been made feasible and are clearly based on the newest technologies in data transfers are of particular relevance and their repercussions need to be meticulously analyzed so that any future legislation can provide realistic answers for them.

---

273 Article 29 Working Party (note 268).
274 *Id.*
275 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri, RAND Europe: Review of the European Data Protection Directive, available at: http://www.rand.org/pubs/technical_reports/TR710.html (13 February 2015.)
276 Borivoje Furht & Armando Escalante, Handbook of cloud computing (2010.)
277 Hunton Privacy Blog (note 269).; European Commission (note 242).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

As it has already been pointed out the 'purpose limitation' principle does not stop to the explicitly defined purposes for which a set of given data are collected, transferred or stored but goes one step further to assess also how compatible are the actual uses effected with a particular set of data compared to the stated ones at the moment of collection.

The framework for the compatibility assessment which answers whether uses of data other than the ones stated at the moment of collection are permissible or not is based on the notion of 'further processing'. A generally acknowledged working definition for this notion is: "...any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility."[278] From here comes another term that needs to be defined, i.e. that of '(in)compatibility'. This notion is understood to suggest that "the fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis."[279] A compatibility assessment can be either a purely formal or a substantive one[280]:

– A formal assessment is suggested that it should compare the purposes that were initially provided, usually in writing, by the data controller with any further uses to find out whether these uses were covered by the initially stated purposes (explicitly or implicitly).
– A substantive assessment should go beyond formal statements to identify both the new and the original purpose, taking into account the way they are (or should be) understood, depending on the context and other factors.

When conducting a compatibility assessment several key factors are suggested to be considered, namely[281]:

– the relationship between the purposes for which the data had been originally collected and the purposes of further processing
– the context in which the data had been collected and the reasonable expectations of the data subjects as to the further use of their data that they agreed to submit to the controller for collection

278 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275).
279 *Id.*
280 Siani Pearson & George Yee, Privacy and security for cloud computing (2013.)
281 *Id.*

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

– the nature of the data and the impact of the further processing on the data subjects
– the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

The newly arriving GDPR tried to settle the above frictions by introducing the 'legitimate interest' concept[282], which tries to make use and processing of data more flexible and pragmatic in light of the technological standards of today by recognizing wider margins of differentiation in the stated purpose for which data are collected between the time of their collection and the time the processing takes place, without, however, going as far as allowing processing of data for purposes totally alien to those at the time of their collection[283]. Despite the fact that this latest regulatory device is indeed heralded by many as a facilitator for the big data and IoT economy[284], there are just as many scholars who point out to the risk that an arbitrary interpretation of the 'legitimate interest' concept may jeopardize

282 Regulation (EU) 2016/679 (GDPR) (note 25); in particular, perambulatory clause no. 47, which reads: "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place..."; also, perambulatory clauses 48, 49 and 50, which aims to retain some of the limitations (i.e. protections) offered to data subjects with the old regime of the DPD by stating: "…such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.".

283 This precarious balance can be observed throughout GDPR's operative clauses regarding the 'legitimate interest' ground, i.e.: Art. 1(f) ["…processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."], art. 13, para. 2(d), art. 35, para. 7(a), to name a few; Regulation (EU) 2016/679 (GDPR) (note 25).

284 Viktor Mayer-Schonberger & Yann Padova, *Regime Change: Enabling Big Data through Europe*, XVII The Columbia Science & Technology Law Review 315–

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

the protection granted so far to data subjects or, at least, it may cause a lot of confusion before the transit from the old to the new regime is completed[285]. It goes without saying that in the meantime technological advancement may have again bypassed regulatory prudence causing a vicious circle, the exit of which can only be achieved if cloud computing regulation stops being so 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.

c. The European Data Protection Directive 95/46/EC; an assessment of its effects on the prevalent views about data protection and related IT technologies; are things different under the GDPR?

In April 2016, the European Parliament and the Council finally reached a conclusion after several years of consultations and negotiations and adopted the General Data Protection Regulation, which is set to become, as of 2018 when it enters into force, Europe's law of reference regarding a wide range of privacy and IT affairs. However, prior to the GDPR, Europe had been handling these affairs based on its world-famous Data Protection Directive or the DPD, as it is often quoted. And despite the fact that the DPD

335 (2016); W. Gregory Voss, *European Union Data Privacy Law Developments*, 70 Business Lawyer 253–260 (2014/2015.)

285 Dutch Lawyers ed., Privacy for the Homo Digitalis. Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (2016); Olof Nyrén, Magnus Stenbeck & Henrik Grönberg, *The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research*, 29 European Journal of Epidemiology 227–230 (2014); Menno Mostert, Annelien L. Bredenoord, Biesaart, Monique C I H & Delden, Johannes J M van, *Big Data in medical research and EU data protection law. Challenges to the consent or anonymise approach*, 24 European Journal of Human Genetics 956–960 (2016); Tobias Bräutigam, The Land of Confusion. International Data Transfers between Schrems and the GDPR; Alexander Roßnagel ed., Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung. Neue Aufgaben und Befugnisse der Aufsichtsbehörden (2017.)

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

will soon cease to apply, its remarkable lifespan makes it a timelessly significant piece of law, whose functions and effects merit careful analysis in the context of a study on cloud computing regulation.

To begin with, after two decades of continuous application, one could generally say that the impact of the DPD on European perceptions of data protection principles has been largely positive. The Directive can fairly be credited for achieving to harmonize and professionalize a core body of data protection principles within Europe, even if implementation still varies from one Member State to the other. The Directive is also generally recognized as a piece of law that created one of the world's leading paradigms for privacy protection, which has served as an inspiration to legal regimes outside Europe. According to the opinions of many academics but also as statistical data suggests[286], EU's DPD has been the reference for the production of data protection legislation by most third countries, apart from the United States and China that have their very own data protection legal cultures.

However, despite this substantially positive impact and general admittance of the soundness of principles behind the Directive, certain aspects have also received considerable criticism which, for the most part, remains relevant even after the adoption of the GDPR given the dynamism with which cloud computing technology continues to evolve. The main objections voiced from within the EU have often focused on the formalities imposed by the Directive (or by its national transpositions across Member States), the economic costs of compliance to the procedures it prescribes and the unequal enforcement from one EU country to another. Compliance costs largely remain an issue under the GDPR as well, especially considering the introduction of the data protection officer as an essential role in the organigram of a great deal of entities dealing with personal data. The unequal enforcement is an issue that is supposed to be resolved when a piece of EU law is elevated from the status of a Directive to that of a Regulation[287]. However, there are numerous voices warning of the reservations the GDPR makes for national regulators, which can be exploited and undermine equal implementation across all EU member states[288]. Outside Europe, many data protection competent organizations tend to perceive the European regulations as somewhat paternalistic towards the respective

286 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275).
287 P. P. Craig & G. de Búrca, EU law. Text, cases, and materials (2015.)
288 Jiahong Chen (note 24).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

laws of third country legal orders or other comparably valid data protection approaches.

One of the most fervently debated points for the DPD was its mechanism for determining and assigning accountability[289]. Overall, it is extremely difficult to infer or even predict how public and private sector bodies that act as data controllers intend to use personal information in the future[290]. Therefore, accountability provisions must be flexible enough to apply in different cases and suit the context in which personal data is used on each occasion. This may be reasonably understood as implying that accountability measures for data controllers with economic drives in mind might need to be different from those for the public sector or individuals, as accountability imposable via economic sanctions can expectedly be more effective in situations where the incentive for personal data processing was generated by pursuance of direct economic benefit. Under the GDPR a step is certainly made towards more efficient accountability allocation not only with economic criteria in mind but also with consideration of the various ways in which data are processed and not just of the entities they run the processing and how financially robust or weak they are, e.g. the possibility to allocate accountability even to algorithms enacting data processing[291]. Nevertheless, the problem of technology-bound regulation persists and further, bolder moves towards more generic rules are necessary.

Just as there have been several pioneering points in the DPD, over the two decades that it has been in force, scholarly opinion and interested bodies have also pointed out certain weaknesses of the Data Protection Directive. The most important ones, which have actually been aggravated with the advancement of new technologies like cloud computing and which pay witness to the need for IT regulation to take the decisive step and more from a perspective anchored to current applications of cloud computing technology to a more generic one that will take into account what the cloud is capable of doing beyond what it is currently doing, were:

– The link between the concept of personal data and the real risks related to data handling, which is no longer clear enough[292]. The DPD was

289 Borivoje Furht & Armando Escalante (note 276).
290 European Commission (note 242).
291 D. Hofman, Duranti L. & E. How (note 4).
292 Siani Pearson & George Yee (note 280).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

conceptualized in an era of plainer, more linear data transfers[293]; today's cloud applications and networks, which are characterized by lack of geographical borders, dynamic handling of resources and a true global nature, have fundamentally altered the standards regarding data handling. The risks that data face today are more complicated and multi-layered, just as more multi-layered are the cloud systems used to handle it.

– The application scope of the DPD largely depended on whether or not the data processed can be defined as "personal"[294]. In fact, provisions of the Data Protection Directive set a 'take it or leave it' setting regarding applicability of what they prescribe to each and every collection of data: there is no room for "more or less personal" data (and, respectively, "more or less protection" of them). However, today's economy has already facilitated the emergence of different types of data, such as anonymous or anonymized big data, data related to state and governance etc.[295]. For these subdivisions of data, the DPD did not provide adequate answers anymore and understandably so given that these data species are products of human activity much more recent than the times the DPD was drafted. As it was just pointed out, the GDPR contains specific provisions for these new typifications of data, yet the issue of excessive anchoring to the current state-of-the-art instead of focusing on technological feasibilities as well persists.
– DPD's measures aimed at ensuring transparency of data processing through better information and notification of data regulators had become inconsistent and ineffective in today's data processing landscape[296]. The privacy policies provisioned by the DPD were no longer matching average data practice. The majority of data handling actions are nowadays carried out by plain consumers, yet the processes prescribed to make these actions secure were highly complex, addressed primarily to law professionals and not average individual users who, nevertheless, should have a clear idea of protective measures in effect[297]. As these non-expert individuals are the direct perpetrators of

293 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275).
294 *Id.*
295 Christopher Kuner, Transborder Data Flows and Data Privacy Law (2013.)
296 European Commission (note 242).
297 International Working Group on Data Protection in Telecommunications (note 265).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

such a significant amount of data processing, they do need to be able to easily comprehend the protective measures which they need to apply or which are in place to protect them. This unanimity in prescribed privacy policies does not really enhance market differentiation, given its stiff, all-or-nothing nature, while it can also be reasonably argued that it hinders fair competition and consumer choice as it sets up very specific standards for market entry to aspiring new service providers. The notification mechanism that the DPD had foreseen was of an unclear purpose[298]: there were as many as 20 different notification processes, and an equally significant variety of exemption rules; at the same time, much of the process was carried out through paperwork or via an awful load of reporting platforms, which are totally incompatible with the rapidness and efficiency that cloud technologies permit today in all data handling processes[299].

– The rules on data export and transfer to third countries, as they were prescribed in the DPD, are nowadays outmoded and out of line with the technological status quo[300]. First of all, the definition of 'third countries' is perceived as outmoded in light of the fact that technological facilities are no longer restricted within the geographical borders of particular countries, let alone within the geographical borders where a service provider has its headquarters. This, in turn, had caused even more complexities as notions like the 'adequacy of countries' is no longer relevant to business realities or data protection, given that the business or the data processing is not carried out necessarily within one and only country anymore. Last but not least, regulation in some other countries is generally admitted to be even stronger than in the EU; however, given the DPD's stiff criteria in its adequacy mechanism (but also, due to other, mainly political or bilateral reasons) these countries were still, till the very last days of DPD's applicability, not recognized as adequate.
– The tools providing for transfer of data to third countries were cumbersome[301], as it has already been pointed out. At the same time, the length of time and effort required to get Standard Contractual Clauses, Model Contracts or Binding Corporate Rules approved was excessive

298 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275).
299 Christopher Kuner (note 295).
300 Borivoje Furht & Armando Escalante (note 276).
301 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

and unrealistic in light of the fast pace at which data handling is carried out via cloud systems today.
– It is beyond the purposes of this paper to examine weaknesses of the current regime that are rooted in factors such as the poor coordination between the Member States, the role of DPAs in accountability and enforcement of the provisions or the uneven implementation of enforcement across Member States or the different criteria for imposing sanctions. However, these too were fair points of criticism against the DPD which should not fail our attention.
– Last but not least, the DPD regime was heavily criticized towards the end of its era on the definition of entities involved in processing and managing personal data it contains as being simplistic and static[302]. Genuinely globalized data transfers[303] and increased re-use of personal data have effectively rendered outmoded the static definitions of data controller and processor of the DPD, calling for a fundamentally new regulatory framework.

As it will be argued immediately after, the GDPR dealt with a fair amount of these shortcomings and criticisms. However, the regulatory challenges posed by cloud computing are from definitively settled with the new Regulation and on the course of this analysis ideas and solutions will be put forward that will hopefully permit a more wholesome take on cloud computing and overall IT regulation in the near future.

d. Focus on the General Data Protection Regulation: is the European Union's brand new law already insufficient to effectively regulate the cloud?

An historical overview on the most important legal texts that have shaped the way EU law is treating the cloud phenomenon today would not be complete without a conclusive reference and analysis on the newly voted and impedingly binding upon all EU Member States General Data Protection Regulation. The GDPR has been adopted recently by the European Union and is expected, as of 2018, to replace the Data Protection Directive. This brand-new piece of EU law deals with all IT applications involving processing of personal data that used to be regulated by way of the

302 *Id.*
303 Christopher Kuner (note 295).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

provisions of the DPD and it is the fruit of yearlong negotiations and consultation processes. Therefore, one would reasonably expect that during the preparatory phase for this new law the particularities of the cloud computing phenomenon had been well taken into consideration and that its provisions are structured in such a way that they can tackle all sorts of legal challenges posed by the cloud. True as that may be – and indeed it is not the intention of this study to argue that the GDPR is of little use before it even enters into force – the overall regulatory framework of EU law in the field of IT law remains incomplete. As it will be argued and thoroughly analyzed at a later stage of this paper[304], the main reason for that is the fact that so far IT laws insist on focusing and regulating applications made possible thanks to cloud technologies but not the cloud phenomenon itself. In other words, all the laws that we currently have on our disposal to provide solutions caused by the IT applications that we are using are absolutely useful and welcome but, as long as we continue to produce or update them having the end cloud-enabled applications that exist on the market in mind, they will just be specialized laws. By 'specialized laws' reference is made to the typification of technology-specific laws, which is of paramount importance in the discipline of IT law[305]. Although it extends beyond the scope of this study to analyze under what criteria a piece of IT legislation or regulatory principle classifies as a technology-specific or technology-generic one, the aim of this project is to propose the methodology with which regulators should work to complement the frameworks of their jurisdictions with basic principles on cloud computing of a technology-generic nature.

304 For more see Chapters 8, 9 and 10.

305 For a more thorough introduction on the issue of technology-specific vs. technology-generic IT laws refer to: Xenofon Kontargyris, From effective to efficient regulation of ICT: time to build the backbone of information technology legislation, available at: http://www.juwiss.de/66-2016/. In addition, for more extensive analysis on the issue look in: V. Sharma, Information Technology Law and Practice (2011); N. Cox, Technology and Legal Systems (2016); Jonathan B. Wiener, *The regulation of technology, and the technology of regulation*, 26 Technology in Society 483–500 (2004); R. Brownsword, E. Scotford & K. Yeung, The Oxford Handbook of Law, Regulation and Technology (2017); S. Brenner, Law in an Era of Smart Technology (2007.)

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

i. Does the GDPR set up a truly universal legal framework for data transfer law?

For starters, it is worth dedicating some attention on the GDPR and discuss some of its inherent deficiencies or failings, which may even undermine its ability to provide for a very long time working solutions to the well-known issues of privacy and security in the field of data transfers, which is its natural field of application anyway. One of the primary points of concern with regard to the efficiency and longevity of the GDPR is the way its makers chose to deal with the issue of territoriality as far as applicable law is concerned. Actually, the Regulation follows a similar pattern to the one implemented by the DPD on this issue; however, unlike the Directive, the issue of applicable national law is no longer addressed at all[306]. On the contrary, the Regulation explicitly permits Member States to deviate from its default rules on a series of specific matters, certain among which have the potential to trigger serious problems concerning the applicability of national data protection laws. What is worse, these potential conflicts of law may be further exacerbated by the tendency of Member State laws to exploit this possibility of unilateral scope definition in incompatible ways, are bound to create legal uncertainties to data subjects, data controllers and data protection authorities[307]. Several scholars are putting forward the idea of resorting to private international law for resolving such conflicts. Nonetheless, handy as it may come in certain cases, private international law can only play a very limited role in this respect due to the unique and bindingly structured nature and objectives of EU data protection legislation. It goes without saying that uncertainties posed by this issue of silence on the topic of territoriality will eventually be clarified by the new European Data Protection Board or the CJEU, but some difficulties are nevertheless bound to persist.

Prima facie, the fact that the GDPR does not contain any reference regarding the relationship between EU and national legislations should sound perfectly reasonable; after all, a Regulation is precisely meant to have direct, universal, and consistent binding force throughout the EU[308]. According to the letter of EU constitutional law, if perfectly implemented,

306 Jiahong Chen (note 24).
307 Ibrahim Hasan, *New EU data protection regulation* Law Society Gazette (2016); Alexander Roßnagel ed. (note 285).
308 P. P. Craig & G. de Búrca (note 287).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

the GDPR should lead to a data protection legal framework that is unanimously applied across all Member States, at least in principle. Consequently, the issue of determining applicable national law would no longer exist as the Regulation would be considered the only valid law on the matter in all EU and EEA jurisdictions. It goes without saying that this was the intention of those that drafted the GDPR and, taking this into account, it appears to be beyond necessary to have provisions on conflict of laws, since the main is let only one law take over anyway. This is most likely why the question of applicable national law no longer shows up in the Regulation and no such reference is to be found. But the question remains whether this EU-wide landscape will indeed be achieved.

In reality, early analysis and review of the provisions of the GDPR suggest that there are at least two areas where national data protection laws will remain relevant even after the Regulation's entry into force. Firstly, the Regulation does not prevent Member States from enacting national provisions with regard to particular issues that are unspecified by the GDPR itself. The most common reason why such issues are not explicitly regulated in the text of the Regulation is the fact that, in relation to several topics, the GDPR has maintained the letter and text of the DPD; although the room for national 'originality' will be narrower due to the binding force of the Regulation compared to the Directive, as long as these issues remain vague, nothing can be taken for granted[309].

Secondly, apart from the grey areas where there is silence from the Regulation on specific matters in the way it was just explained, there are some other issues on which, even more importantly, the Regulation explicitly permits Member States to decide whether they wish to deviate from its own provisions on certain aspects. In particular, Recital 8 of the GDPR reads: 'Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation…

309 An extensive analysis of all concepts and ideas in the field of data protection law that are even somewhat differently defined across different national EU laws can be found in: European Commission, Working Paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments (2010.)

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of sensitive data…'[310]

This excerpt reflects then in the provisions of Article 6(1) [in particular, points (c) and (e)] and Article 9 of the operative part of the GDPR. Article 6(1) is where the legal grounds on which processing of personal data can be legitimized are stipulated. Point (c) provides that processing is considered legal if it 'is necessary for compliance with a legal obligation to which the controller is subject'[311]. In the same spirit, point (e) permits processing that 'is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'[312]. Further down, in Article 6(3) the GDPR elaborates that the two previous legal bases must be provided for by either 'Union law' or 'Member State law to which the controller is subject'[313]. As far as Article 9 is concerned, the GDPR therein attempts to set a higher threshold for the processing of sensitive data by imposing a prohibition on operations over these categories of personal data, unless one of the exceptions it stipulates applies[314]. In similarity to what happens in Article 6(1), this provision also gives Member States a sideway regarding a few matters, as it can be verified by reading its text. Each of these provisions could potentially set fertile ground for a conflict of laws between two or more Member States.

ii. What does the spirit of GDPR tell us about the longevity of the current overall EU data protection regime?

It is admittedly a bit early to bring out strong verdicts on how good or bad the GDPR will turn out to be as a piece of legislation. However, while waiting for the new law to enter into force and start producing real regulatory output so that we can evaluate it as positive and efficient or negative and insufficient, we can already draw certain conclusions regarding the dynamism and rejuvenation that this major uplift of EU data protection law, which has been attempted with the adoption of the GDPR, does indeed carry. And, in this context, it has to be pointed out that the GDPR is

310 Regulation (EU) 2016/679 (GDPR), Recital 8 (note 25).
311 Id,, art 6(1)(c) (note 25).
312 Id,, art 6(1)(e) (note 25).
313 Id,, art 6(3) (note 25).
314 Id,, art 9 (note 25).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

expected to achieve very little with regard to reviving the long-stagnated data protection regime of Europe. This is so due to the fact that the three main aims that the GRDR sets for itself are based on unrealistic assumptions[315].

The first wrongful impression is the persistent one, at least in Europe, that data protection law can offer to individuals actual control over their data, which it cannot[316]. The second is the popular belief that the recent reform has managed to simplify the law, while in fact it has only made compliance even more complex. And last but not least, comes the assumption that data protection law should be comprehensive, while, as it has also been previously discussed, data protection is an issue raised by specific IT end applications only and, therefore, it can only provide footing for technology-specific legislation. We cannot stretch data protection laws to regulate every single issue raised by IT as a whole, because then we drain the originality out of it causing only confusion and legal uncertainty. In detail:

– Shortcoming no. 1: too much obsession with data self-determination

Although data protection is in no way synonymous with the unequivocal ability to decide alone on the destiny of any kind of data referring directly or indirectly to you, in European legal thinking and practice the two concepts have persistently been brought forward as concurrent. 'Informational self-determination' is the most widely-used term to describe the notion that people should be able to exercise control over what happens with their personal data[317]. This concept implies, on the one hand, that individuals' free and informed consent is an important element towards legitimizing data processing, and, second, that individuals have various and very pluralistic in content rights by which they can exercise control over the data, such as rights to correction or erasure.

Viewed through the prism of today's technological status quo, the idea of consent is largely a fallacy[318]. Yes, consent may be considered within a great number of contexts as a typical way for individual data owners to fa-

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

316 See also Chapter 3.

317 W. K. Hon, C. Millard & I. Walden (note 119); Steffen Kroschwald ed., Informationelle Selbstbestimmung in der Cloud. Datenschutzrechtliche Bewertung und Gestaltung des Cloud Computing aus dem Blickwinkel des Mittelstands (2016.)

318 See also Chapters 2 and 8.

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

cilitate or block data processing; but in light of today's status quo, this is now largely theoretical and with little practical meaning, if any at all.

For the greatest number of services where personal data are involved, often, there is little room for choice: if you want to use a service, you have to comply with the technical conditions its maker or provider has built it upon — which may well entail giving in certain personal data. Otherwise, access will be simply denied, not because the specific service provider is not interested in profit or increasing the market of their service but because the service simply cannot work otherwise[319]. In addition, it needs to be pointed out that, while it gets more and more popular to work on ever more simplified ways for IT applications users to express consent, this works to the detriment of meaningful consent. The fact that a user of a data-related service ticks a box next to a statement of consent after having viewed some brief and simplified imagery roughly describing the kind of consent they are about to give does not mean, of course, that they have sincere knowledge over the kind of permission they are giving[320].

What is more, technological reality of the 21st century tends to erode or progressively invalidate any giving of consent. Even if a data owner expressly permitted certain uses of their information at some point, technological practices such as databases, profiling, and Big Data make informational self-determination all the more elusive[321].

Last but not least, even if we accept that informational self-determination can function effectively in the context of private relationships and applications or services – and to a very significant degree, it does function – it works poorly or it is not even supposed to apply in many cases when it comes to citizen–government affairs[322]. Citizens exercising control over the fate of their personal data, which is what informational self-determination is all about, contrasts with the character of many data-driven applications from the public sector[323].

---

319 Solon Barocas & Helen Nissenbaum eds., On Notice: The Trouble with Notice and Consent (2009); Alexander Roßnagel ed. (note 285).

320 Solon Barocas & Helen Nissenbaum eds. (note 319).

321 Viktor Mayer-Schönberger & Kenneth Cukier, Big data. A revolution that will transform how we live, work, and think (2013.)

322 A. Froomkin, *Of Governments and Governance*, 14 Berkeley Technology Law Journal 618–633 (1999.)

323 Kristina Irion (note 220).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

– Shortcoming no. 2: taking controllers' due diligence too much for granted

The current data protection regime not only relies too much on user permission, but also on the assumption that data controllers are duly fulfilling their duties, either because they feel obliged to do so from the presence of Data Protection Authorities or because they deliberately choose to be diligent[324]. And it is true that, some notorious exceptions aside, for most undertakings and organizations dealing with data, legal compliance is of paramount value. However, even if we assume that all kinds of data controllers want to observe data protection law, it cannot be taken for granted that they are in a realistic position to do so. To begin with, controller compliance is undermined by the fact that data protection law is complex to put from theory to practice. Moreover, 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[325].

– Shortcoming no. 3: excessively outstretching statutory data protection laws to the extent that they become dysfunctional

As it has been analyzed both the GDPR and its predecessor, the DPD, are pure examples of technology-specific laws. They determine how the issues they deal with are to be regulated by focusing on the results data technology has when applied in the context of specific data services or for the completion of particular data-related tasks. This is an understanding we need to keep in mind at all times when reading a statutory law such as the GDPR, which, in addition, has been constructed in light of a particular factual framework (e.g. the reality of transborder data transfers). Very of-

324 B.-J. Koops (note 315); Alexander Roßnagel ed. (note 285).

325 See also Chapters 8, 9 and 10.

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

ten, expanding the meaning of the provisions of a statutory law, which is, nevertheless, of a technology-specific nature, to such an extent that is can cover more and more novel phenomena caused much more legal confusion and uncertainty than it actually resolves[326]. In other words, what needs to be done is to stop abusing technology-specific IT laws, such as the GDPR and the like, in order to continue being on a relative par with technological advancement and novel IT applications and focus on conceptualizing robust regulatory principles reflecting on the core and heart of modern and future IT, i.e. on cloud computing.

e. GDPR and its readiness to respond to big scale uses of data in the cloud; the case of machine learning

Just as the GDPR was going through its negotiations phase, the cloud was becoming the platform for numerous big scale data-based applications which are becoming increasingly important in several aspects of the internet-based economy[327]. The majority of them are founded on processing of data of massive amounts, typically being referred to as 'big data'[328]. Most, if not all of these uses, are made possible thanks to cloud computing and,

326 Colin S. Diver, *Statutory Interpretation in the Administrative State*, 133 University of Pennsylvania law review 549–599 (1985.)

327 See also Chapter 11.

328 Big data is an evolving term that describes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information. Big data is often characterized by three qualities, which in relevant technical literature have been established as 'the 3 Vs': extreme **volume** of data, wide **variety** of data types and **velocity** at which the data must be processed. Although big data does not equate to any specific volume of data, the term is often used to describe terabytes, petabytes and even exabytes of data captured over time. Such voluminous data can derive from countless different sources, such as business sales records, harvested results of scientific experiments or real-time sensors used in the internet of things. Data may be raw or preprocessed using separate software tools before analytics are applied. It may also exist in a wide variety of file types such as structured data, e.g. in SQL database stores; unstructured data, e.g. document files; or streaming data from sensors. Moreover, collection of big data may involve multiple, simultaneous data sources, which may not otherwise be integrated. Velocity refers to the speed at which big data must be analyzed. As a rule, every big data analytics project will ingest, correlate and analyze data sources, and then render an answer or result based on an overarching query. This means that for the final product of the processing to be of essence, human ana-

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

naturally, will clearly be within the field of application of the GDPR. The aim of such massive data processing operations can be greatly diversified but one of the most common purposes they serve is to create patterns that will be able to predict human behavior, choices and decisions[329]. These patterns are then fed to systems such as online marketplaces or software and systems used in tracking health of patients or dissemination patterns of diseases, to name a few. Moreover, the bigger the amount of data collected and processed, the more accurate these patterns are supposed to become and the more precise the predictions they render[330].

It goes without saying that one of the biggest questions surrounding the GDPR is to what extent the new law has managed to be timely enough when it was officially adopted in order for its provisions to regulate these phenomena efficiently for as long as possible. Of course, this question is too broad one for it to merit a mere 'yes' or 'no' answer. However, an as-

---

lysts must have a clear understanding of the available data and possess some sense of the kind of answer they are looking for. Velocity becomes of growing importance as big data analysis expands into fields like machine learning and artificial intelligence, where analytical processes mimic perception by finding and using patterns in the collected data. Achieving such velocity in a cost-effective manner is a major challenge. Even enterprise leaders are reticent to invest in an extensive server and storage infrastructure that might only be used occasionally to complete big data tasks. Consequently, public cloud computing has emerged as a primary vehicle for hosting big data analytics projects. A public cloud provider can store petabytes of data and scale up thousands of servers just long enough to accomplish the big data project. The business only pays for the storage and compute time actually used, and cloud instances can be turned off until they're needed again. For more details and orientation into the concept of big data, refer to: Viktor Mayer-Schönberger & Kenneth Cukier (note 321).; Jonathan Stuart Ward & Adam Barker, Undefined By Data. A Survey of Big Data Definitions, available at: http://arxiv.org/pdf/1309.5821; Amir Gandomi & Murtaza Haider, *Beyond the hype*. *Big data concepts, methods, and analytics*, 35 International Journal of Information Management 137–144 (2015); Andrea de Mauro, Marco Greco & Michele Grimaldi, *What is big data? A consensual definition and a review of key research topics*, in, 97–104 (2015); Ibrahim Abaker Targio Hashem, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani & Samee Ullah Khan, *The rise of "big data" on cloud computing*. *Review and open research issues*, 47 Information Systems 98–115 (2015).

329 Dimitra Kamarinou, Christopher Millard & Jatinder Singh, Machine Learning with Personal Data (2016.)

330 Andrej Savin, *Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks* SSRN Journal (2014); Alexander Roßnagel ed. (note 285).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

sessment can indeed be driven for the issue of machine learning given the specialized provisions on profiling[331] that form part of the GDPR.

As a rule, automated decision-making[332] often entails profiling, where the profiles gradually constructed through the processing of data guide the decision-making process[333]. Reflecting this technological fact, the GDPR defines profiling as a sub-category of automated processing, and stipulates it as the use of personal data to evaluate certain personal aspects of natural people in an effort to analyze and predict certain aspects of their behavior.

In the era of the DPD already a number of academics had suggested that one of the Directive's underlying principles was that 'fully automated assessments of a person's character should not form the sole basis of decisions that significantly impinge upon the person's interests'[334]. This principle survives in the provisions of the new Regulation, where according to its Article 22 – which also covers profiling of people based on their health, location and movement – data subjects have the right not to be subject to decision-making if that is solely based on automated processing, at all instances that this may significantly affect them in some way. This provision plays a crucial role in relation to machine learning, given that proponents of the specific technology emphasize precisely its ability to automate and facilitate decision making processes.

The rest of protection mechanisms, appeal processes and risk assessment or control procedures of the GDPR can naturally be read through the prism of profiling as well, given its explicit recognition as a form of data processing that falls within its regulatory scope from the GDPR[335]. It is beyond the scope of this study to analyze the entire body of provisions of the new Regulation; however, if one conclusion is to drawn regarding big scale data processing operations which are made possible thanks to cloud

331 In particular, Art. 4, para. 4, and Art. 22, Regulation (EU) 2016/679 (note 25).

332 The term 'automated decision making' refers to the use of computers to carry out tasks requiring the generation or selection of options. For further details refer to: McGraw-Hill, McGraw-Hill Dictionary of Scientific and Technical Terms (2003.)

333 Andrej Savin (note 330).

334 Lee A. Bygrave, *Aytomated Profiling*, 17 Computer Law & Security Review 17–24 (2001.)

335 Profiling is explicitly mentioned in all instances of GDPR rules where specific protective measures and tools available to data subjects are stipulated, namely: Art. 13, para. 2f; Art. 14, para. 2g; Art. 15, para. 1h; Art. 21, para. 1 & 2; Art. 35, para. 3a; Art. 47, para. 2e Regulation (EU) 2016/679 (GDPR) (note 25).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

computing (such as profiling and, subsequently, machine learning), it can be argued that EU data protection law, in its latest form, still assumes that large scale data applications such as automated decision-making processes are risky and that individuals need to be protected from them. Among the types of protection granted to data subjects are the right to be informed about automated decision-making, including profiling, as well as rights to have a human review a machine decision. While such measures are indeed useful to be in place and uphold Europe's long tradition of empowering the individual against undesirable uses of their data, as much as possible, enthusiasts of relevant technologies (the cloud being one of them) point out that technology should not always be viewed with suspicion[336]. For instance, advances in machine learning research and in cloud networks as the main enabler of machine learning systems, mean that machines can more and more may surpass certain limitations of human decision makers and provide us with decisions that are emphatically fair[337]. How 'ready' is the GDPR to show tolerance and trust towards these technologies and their constantly improved capabilities? Time and actual enforcement practices of the new law by competent authorities will soon tell us.

f. Vision for a cloud-based future

It has already been demonstrated that today data is prevalent everywhere. Sources of data are multiple in comparison to a couple of decades ago, their uses are also many more, their economic value is incomparably higher than it used to be and from the moment they are collected, data venture on an open-ended journey through multiple uses, different formats and several platforms. With this landscape in the field of data in mind, a very different privacy framework for the data age is necessary, one focused less on individual consent at the time of collection and more on continuously holding data users, be them controllers or processors as they are typified for the time being, accountable for what they do with the information they have in their possession[338]. Under such a regulatory regime, entities that have any kind of data in their possession will formally assess any particular use or reuse of them based on the impact it has on the individuals these

336 Jiahong Chen (note 24).; Andrej Savin (note 330).; B.-J. Koops (note 315).
337 Dimitra Kamarinou, Christopher Millard & Jatinder Singh (note 329).
338 For more see Chapter 8.

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

data originally belong to or come from. This perpetual accountability does not have to be onerously detailed or excessively time-consuming[339]. 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. In general, the cloud and the IT environment it fosters call for a regulatory framework that will spur creative services for, uses and reuses of data, while at the same time it will ensure that sufficient measures are taken[340] to make sure individuals, who data belong to or come from, are not hurt.

g. The road from data privacy to cloud computing regulation

i. Privacy and security viewed through the years and across major jurisdictions[341]

Viewed from a European standpoint, privacy has been traditionally regarded as a fundamental human right. Enshrined in the United Nations Universal Declaration of Human Rights (1948)[342], it subsequently became part of the European Convention on Human Rights[343] and numerous national constitutions and charters of rights across Europe but also worldwide[344]. Since

339 For more see Chapter 10.
340 For more see Chapters 8, 9 and 10.
341 Siani Pearson & George Yee (note 280).
342 Article 12 of the UN Universal Declaration of Human Rights reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.". UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
343 Article 8 para. 1 of the ECHR reads: "Everyone has the right to respect for his private and family life, his home and his correspondence.". Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.
344 For an extensive overview of the basic privacy laws and regulations across most countries around the world, refer to http://privacypolicies.com/blog/privacy-law-by-country/ (last accessed: 01/19/2017.)

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

at least the 1970s, the primary focus of privacy had been personal information particularly that which was put under question from government surveillance or potential mandatory disclosure in light of the need to set up databases on topics of public security, health or other emergencies.

The 1980s brought along the rise of direct marketing and telemarketing[345] and, consequently, new kinds of concerns were raised related to privacy of personal data and security, while soon after the transposition of buying and commerce on the internet spurred further consideration to the increasing threats of online identity theft and spamming[346].

In the end, one could argue that one way of thinking about privacy is as 'the appropriate use of personal information under the circumstances'[347]. Data protection is the management of such personal information and it is a terminology often used within the European Union with reference to privacy-related laws and regulations. On the contrary, in the USA the term 'data protection' mostly refers to security[348].

The terms 'personal information' and 'personal data' are commonly used within Europe and Asia; in the USA, the respective term is 'Personally Identifiable Information' (PII), but, as convergence of jurisdictions as a result of the globalized structures of today's world moves on, the same terms are generally used also in America to refer to the same (or a very similar) concept[349].

The European Union definition of 'personal data', since long established via the DPD, is that of "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[350].

Traditionally, scholarly views tend to differ about certain types of personal data which are considered more sensitive than others; expectedly, these variations occur as a result of the differences in the definition of

345 Bradley, A. K. (1991). An employer's perspective on monitoring telemarketing calls: Invasion of privacy or legitimate business practice? Labor Law Journal, 42(5), 259. Retrieved from https://search.proquest.com/docview/1290705829?accountid=11262 (last accessed: 01/19/2017.)

346 Huaiqing Wang, Matthew K. O. Lee & Chen Wang (note 12).

347 Siani Pearson & George Yee (note 280).

348 C. J. Bennett (note 194).

349 Borivoje Furht & Armando Escalante (note 276).

350 Directive 95/46/EC (DPD) (note 143.)

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

what is considered sensitive personal information from one jurisdiction to the other.

As opposed to Europe's, the US approach to privacy legislation is historically sector-based or enacted at the state level (e.g. the State of Massachusetts has set out appropriate security standards for protecting the personal information of residents of that state) and imposes few if any restrictions on transborder data flow[351].

To summarize, privacy is essentially regarded as a human right in Europe; on the contrary, in America, it has been traditionally viewed more as a concept aimed at avoiding harm to people in specific contexts[352]. It is a complex but important notion, and correspondingly, the collection and processing of personal information is subject to regulation in many countries across the world. As a result, any future set of rules for cloud business will need to reflect these varied perspectives and try to balance among or, ultimately, merge them; and this is a policy recommendation that should be taken into account by regulators in both jurisdictions.

ii. Privacy issues particular to cloud computing technologies

The specificities of cloud technologies and the differences they have introduced in the field of data handling have, subsequently, also modified the challenges that privacy faces in today's IT landscape[353].

For starters, handling your data via cloud means a great lack of user control[354]. User-centric control seems essentially incompatible with the cloud: as soon as a SaaS environment is used, the service provider becomes responsible for storage of data, in a way in which visibility and control is limited. As a result, unauthorized secondary usage of data, risks to data integrity owing to complexity of regulatory compliance or the efforts in addressing transborder data flow restrictions are always possible.

Legal uncertainty is one more direct effect of the rapid development of the cloud sector[355]. Since cloud technology has moved ahead of the law,

---

351 See also Chapter 3.
352 Id.
353 Siani Pearson & George Yee (note 280).
354 Borivoje Furht & Armando Escalante (note 276).
355 Digital Agenda in the Europe 2020 strategy (note 241); Reinhard Posch (note 240).

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

there is understandably much legal uncertainty about privacy rights in the cloud and it is becoming more and more prevalent that applying existing laws to cloud environments gives insufficient results. Cloud computing poses significant challenges for organizations that need to meet various global privacy regulations at the same time, due to the universal nature of IT as a market and its collision with geographical or jurisdictional borders that exist in the real world.

Security issues are also raised due to the emergence of cloud computing[356]. Security gaps, instances of unwanted access or vendor lock-in, inadequate deletion of data, potential compromise of the management interface that would extend to a degree beyond the average user's control or understanding, backup vulnerabilities, isolation failure, inadequate monitoring are just a few situations that could jeopardize the security of cloud platforms and merit attention.

iii. Why does cloud computing call for a new regulatory framework?

It has been already sufficiently demonstrated that cloud computing, from a technological perspective, is fundamentally different from what existed before[357] as tools to perform computational processing of data tasks. Similarly, there are essential differences on the focus of cloud technologies in comparison to previous environments: while systems based on technologies prior to the cloud where largely one-dimensional and they were built more or less on a linear logic and architecture (in the sense that the processing was easily traceable at all times throughout the system, regardless of whether the resources of the system were all in the same physical location or not), cloud environments obey to a multi-dimensional logic: the processing work can be executed using resources dispersed around the cloud facility and without even being at the same physical location either.

Understandably, this shift in the way data processing environments are constructed resulted also in a shift on the priorities they set: 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

356 Borivoje Furht & Armando Escalante (note 276).
357 See Chapter 2.

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

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

In the following parts of this study it will be examined to what degree using the criterion of 'legitimate scope' (teleological perspective) in order to define the justifiable actions of each actor in a data processing workflow facilitated by cloud infrastructure would be a viable norm in order to produce an efficient regulatory framework for cloud computing technologies and the tasks carried out through them. Moreover, recognizing the boundless nature of the cloud, effort will be made to set up this set of regulatory principles with a universal perspective. Consequently, from the one hand, the best possible regulatory approaches will be looked for across the two most predominant markets and jurisdictions where the cloud business thrives, i.e. Europe and the U.S.A. Simultaneously, the proposed scheme will in as much as possible be fit for 'universal applicability', i.e. without being affected by the cross-country or cross-market nature of cloud environments but, instead, by focusing on the cloud infrastructure as a locus in itself, where certain rules should apply and specific regulatory goals and priorities should at all times be respected.

https://doi.org/10.5771/9783845295626-89, am 03.08.2024, 04:17:43
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb