Market and Competition Law Review / VOLUME II / No. 2 / OCTOBER 2018

Cybersecurity and Liability in a Big Data World*

*Maria Lillà Montagnani***
*Mirta Antonella Cavallo****

ABSTRACT: The interplay between big data and cloud computing is at the same time undoubtedly promising, challenging and puzzling. The current technological landscape is not without paradoxes and risks, which under certain circumstances may raise liability issues for market operators. In this article we illustrate the several challenges in terms of security and resilience that market operators face as their overcoming is of strategic importance for businesses wishing to be deemed privacy-respectful and reliable market actors. After a brief overview of the potentialities and drawbacks deriving from the combination of big data and cloud computing, this article illustrates the challenges and the obligations imposed by the European institutions on providers processing personal data – pursuant to the General Data Protection Regulation – and on providers of digital services and essential services – according to the NIS Directive. We also survey the European institutions' push towards the development and adoption of codes of conduct, standards and certificates, as well as their last proposal for a new Cybersecurity Act. We conclude by showing that, despite this articulate framework, big data and cloud service providers still leverage on their strong market power to use "contractual shields" and escape liability.

KEYWORDS: Big data, security, liability, NIS Directive, GDPR, cloud, ISP, Cybersecurity Act

---

* Date of reception: 18 July 2018. Date of acceptance: 15 August 2018.

** Maria Lillà Montagnani is a Professor of Commercial Law, Bocconi University of Milan, 20136 Milan, Italy. lilla.montagnani@unibocconi.it.

** Mirta Antonella Cavallo is a Research Fellow, ASK Bocconi Research Center, 20136 Milan, Italy. mirta.antonella.cavallo@gmail.com.

1. Introduction: new technology trends in a big data world

Unprecedented proportions of digital data, combined with increasingly-sophisticated computation and automation techniques, enable to unveil aspects of personal life that one might rather keep private, but also the prediction of behaviours and events, unknown even to the concerned individuals.[1] Credit card companies are allegedly able to identify customers in love, those who have recently moved into a new home, and even predict an imminent divorce. Similarly, combining patient records with data collected from wearable devices and sensors could help identify (and address) illnesses beforehand.[2] Profiling is now so sophisticated it enables the identification of users' personality and mood, as well as the specific situations they live, through the combined collection and analysis of their browsing activities, the browsing speed, the time spent online and so on.[3] This ever-increasing trend will be amplified as soon "[e]very animate and inanimate object on earth will ... be generating data, including our homes, our cars, and yes, even our bodies".[4] The growing interaction between the physical world and devices such as cars, refrigerators and pacemakers opens up unprecedented possibilities. The Internet of Things (IoT) has already been superseded by the Internet of Everything,[5] and it is expected that by 2021 there will be 11.6 billion mobile-connected devices,[6] with data traffic on mobile network that in 2012 was already at least twelve times larger than Internet traffic.[7]

This new industrial revolution, which is leading to new products, services and business processes, but also shaping social and cultural habits,

---

[1] Although the work is the result of joint reflection, sections 1 and 2 are written by Maria Lillà Montagnani, and sections 3 to 5 by Mirta Antonella Cavallo.
Meredith A. Barrett, Olivier Humblet, Robert A. Hiatt, and Nancy E. Adler, "Big data and disease prevention: from quantified self to quantified communities", *Big Data* 1 (2013): 168-175.

[2] *Ibid.*

[3] Primavera de Filippi, "Big data, big responsibilities", *Internet Policy Review* 3 (2014): 1-12.

[4] Rick Smolan and Jennifer Erwitt, *The Human Face of Big Data* (China: Against All Odds Productions, 2012), 3.

[5] Dave Evans, "How the Internet of Everything will change the world ... for the better #IoE", 7 November 2012, https://blogs.cisco.com/digital/how-the-internet-of-everything-will-change-the-worldfor-the-better-infographic.

[6] Cisco, "Visual networking index: Global mobile data traffic forecast update 2016-2021", 28 March 2017, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[7] Neil Richards and Jonathan King, "Three paradoxes of big data", *Stanford Law Review online* 66 (2013): 41-46, in particular 42.

could be said to be driven by the following – interrelated – emerging technological trends: (i) mobile Internet, through smartphones and tablets; (ii) big data; (iii) cloud computing; (iv) the Internet of Things, relating to the integration between the physical reality and the digital one; (v) artificial intelligence, with thinking and learning machines simulating how humans act;[8] (vi) brain-computer interfaces, which connect external computer devices to the human brain or nervous system to assist individuals' cognitive and motor functions; (vii) near-field communication (NFC) payments, which rely on wireless communication to facilitate financial transactions at points of sale; (viii) mobile robots, which are increasingly able to perceive, reason and act, autonomously or semi-autonomously; and (ix) quantum computing, which applies the laws of quantum mechanics to process large volumes of information much more efficiently than ever before.[9]

While most of these advancements are still at an early stage of development, big data and cloud computing stand out as being the common denominator.

Big data is a catch-all term that has been defined in various ways over time: from a technical perspective, it refers to high-volume, high-variety and high-velocity data assets that enable enhanced decision-making.[10] In other words, big data consists of large amounts of data, different in nature and source – may that be people, machines or sensors – that is generated and processed at an ever-increasing speed and – through sophisticated analysis – from which value is generated and extracted.[11] It is not just about the quantity of data, but also about their increasing variety – in terms of

---

[8] On this, among others, Trevor Bench-Capon *et al*., "A history of AI and Law in 50 papers: 25 years of the international conference on AI and Law", *Artificial Intelligence and Law* 20 (2012): 215-319; Sean Semmler and Zeeve Rose, "Artificial intelligence: Application today and implications tomorrow", *Duke Law & Technology Review* 16 (2017): 85-99.

[9] Benoit Dupont, "The cyber security environment to 2022: Trends, drivers and implications" 2012, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208548, where each trend is explained in detail, with specific regard to the development drivers and the implications for cybersecurity.

[10] This is known as the "3-V" definition model (Volume, Variety and Velocity). On this, Richards Neil and Jonathan King, "Big data ethics", *Wake Forest Law Review* 49 (2014): 393-432, in particular 394.

[11] European Data Protection Supervisor (EDPS), *Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, Opinion 7/2015, 19 November 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2 015/15-11-19_Big_Data_EN.pdf: 5.

format, nature and sources – and processing speed, as well as its potential for effective predictions and often surprising insights.

"We are on the cusp of a 'Big Data' Revolution"[12] which is just the latest stage in the wider information revolution leading to a greater scale of change at a greater speed. In the era of big data, each second massive quantities of data are produced by and about people, devices and their interaction, ranging from purchase history and social media behaviour to phone logs, from health records to genetic sequences. On the basis of big data, algorithms work as "somewhat a modern myth",[13] competing to become part of our daily lives and homes, even able to write "symphonies as moving as those composed by Beethoven".[14]

Indeed, big data could also be defined in terms of the great societal impact it could have, as referring "to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more".[15]

In the context of the collection of increasing complex volume of (big) data and its automated analysis, for algorithms to extract large-scale patterns in human behaviour and reach sophisticated conclusions, it is necessary to rely on a flexible and scalable infrastructure: cloud computing.[16]

Cloud computing has indeed the potential to yield significant benefits, by offering – upon request – continuous and convenient access from anywhere to a pool of resources in data centers equipped with increasingly high computational capacity.[17] More specifically, cloud computing operation (and success) is based on five characteristics: (i) broad network access by a variety of devices and workstations worldwide; (ii) on demand

---

[12] Neil and King, "Big data ethics", 393.

[13] Solon Barocas, Sophie Hood, and Malte Ziewitz, "Governing algorithms: A provocation piece", 29 March 2013, http://governingalgorithms.org/resources/provocation-piece/.

[14] *Ibid*., referring to Christopher Steiner, *Automate This: How Algorithms Came to Rule Our World* (London: Penguin, 2012).

[15] Neil and King, "Big data ethics", 394, referring to Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (New York: Houghton Mifflin Harcourt, 2013).

[16] John Gantz and David Reinsel, "Extracting value from chaos", *International Data Corporation*, 2011, https://uk.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf.

[17] Nicole Lazar, "The big picture: Big data hits the big time", *Chance* 25 (2012): 47-49. See also Lee Badger *et al*., "Cloud computing synopsis and recommendations. Recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology (2012).

self-service, whereby users can enjoy cloud computing resources whenever they so request through a web-based self-service portal and without the need of human interaction; (iii) payment measured on use; (iv) resource pooling, whereby multiple users are served through the same physical resources while data remain securely separated on the logical level; and (v) rapid elasticity that ensures the user to have always the exact capacity it needs at any given time.[18]

Accordingly, at European Union level a cloud computing service is defined as "a digital service that enables access to a scalable and elastic pool of shareable computing resources".[19] To this regard, and to use the words of the European legislator, "the term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment".[20]

Depending on the deployment model, clouds can be structured as: (i) private, when the service is for the exclusive use of a user; (ii) public, when open use by the general public is allowed, and (iii) hybrid, when a mix of both applies.

In order to provide cloud services to users – may that be consumers or businesses –, a provider (hereinafter "cloud service provider" or "CSP") deals with: (i) the implementation of the services, (ii) the abstraction of resources, (iii) the provision of physical resources, (iv) the management of services, and (v) the compliance with security and privacy obligations.[21]

---

[18] Edwin Schoutem, "Cloud computing defined: Characteristics & service levels", *IBM*, 31 January 2014, https://www.ibm.com/blogs/cloud-computing/2014/01/31/cloud-computing-defined-characteristics-service-levels/.

[19] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, 1-30 ("NIS Directive"), Article 4, no. 19.

[20] NIS Directive, Recital 17.

[21] "The implementation of the services" consists in the provision of one of the service models, while "the abstraction of resources" entails the provision of interfaces for interaction, "the provision of physical resources" relates to hardware, and "service management" includes the provision of

Pursuant to a different – but complementary – criterion, cloud services can also be distinguished on the basis of the service model: while Infrastructure as a Service (IaaS) offers processing and storage capacity to users accessing directly from the Internet, as well as the ability to access, monitor, and manage remote datacenter infrastructures (e.g., Amazon Web Services, and Microsoft Azure), Platform as a Service (PaaS) enables users to develop, test, and deploy applications easily through a self-service portal and other instruments provided by the CSP, without the need to install any program into their computers (such as Google Apps Premier, and Google Docs), and, lastly, Software as a Service (SaaS) uses a software – which is centrally hosted – which is licensed to users on subscription basis (e.g., Slack, Dropbox and Concur).

Against this backdrop, we briefly overview the potentialities and drawbacks deriving from the combination of big data and cloud computing, to then focus on security and resilience as of fundamental strategic importance for businesses wishing to be deemed privacy-respectful and reliable market actors. Although the European legislator imposes increasingly strict obligations on providers processing personal data – pursuant to the General Data Protection Regulation[22] – and providers of digital services and essential services – according to the NIS Directive –, encourages their participation in the development of codes of conduct, standards and certificates, and proposes a new Cybersecurity Act,[23] big data and cloud service providers leverage on their strong market power to use "contractual shields" and escape liability.

---

business support, as well as portability and interoperability functions. Lastly, "compliance with security and privacy obligations" depends on the requirements set under the relevant legal system. On this, Ali Gholami and Erwin Laure, "Big data security and privacy issues in the cloud", *International Journal of Network Security & Its Applications* 8 (2015): 59-79, in particular 59.

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, in short GDPR), OJ L 119, 4.5.2016, 1-88.

[23] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "European Union Agency for Cybersecurity", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification, 29 May 2018, 9350/18 ("Cybersecurity Act").

2. Risks and opportunities at the crossroad between big data and cloud computing

Debates around emerging technologies are often heated. Besides the discussion on the nature of technology – good, bad or neutral – its interaction with the social ecology is such that "technical developments frequently have environmental, social, and human consequences that go far beyond the immediate purposes of the technical devices and practices themselves."[24] For instance, "like other socio-technical phenomena, Big Data triggers both utopian and dystopian rhetoric". On the one hand, Big Data is a powerful tool to address various societal ills, offering the potential of new insights into areas as diverse as cancer research, terrorism, and climate change. On the other hand, Big Data is also seen as a troubling manifestation of Big Brother, enabling invasions of privacy, decreased civil freedoms, and increased state and corporate control.[25] As a matter of fact, potentials and risks related to big data and cloud computing are probably only partially known and over time further implications will emerge.

As for the benefits, it is not just about the reduced costs deriving from the use of third-party infrastructures for storing and processing data: according to the enthusiasts, big data are of fundamental importance in preserving and managing valuable resources, curing lethal diseases, and making life safer and more efficient. Those who believe in the "quantified self" welcome tools to measure life and improve sleep, lose weight, be more fit and so on.[26] It is particularly promising that, through big data, it is now possible to establish new correlations between different datasets, so as to infer additional information, predict behaviours and evaluate the probability that a given event will occur.[27] This is particularly useful for businesses, given that the data collected from users – may them be actual or prospect clients – is used to better understand their preferences and behaviour, predict purchases and better direct marketing efforts.[28]

---

[24] Melvin Kranzberg, "Technology and history: Kranzberg's laws", *Technology and Culture* 27 (1986): 544-560, in particular 545.

[25] Danah Boyd and Kate Crawford, "Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon", *Information, Communication & Society* 15 (2012): 662-679, in particular 663-664.

[26] Neil and King, "Big data ethics", 41.

[27] Bill Franks, *Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics* (New Jersey: John Wiley & Sons, 2012), 49.

[28] Michael J. Berry and Gordon S. Linoff, *Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management* (New Jersey: John Wiley & Sons, 2004).

Not surprisingly, tailored services are increasingly being developed and targeted advertising has become a common practice among businesses. Aggregation, use and reuse of data are now an essential part of many business models, to the point that data has been labeled as the "oil"" of the 21st century.[29] Accordingly, it is not surprising that the cloud computing market is projected to reach $411 billion by 2020.[30]

At the same time, big data raises numerous risks that are, at least initially, well exemplified in the "three paradoxes" identified by Richards and King.[31] Firstly, it should be noted that big data concerns all kinds of private information, while the systems and techniques used for processing are generally under legal and commercial secrecy. This is known as the "transparency paradox". Secondly, it is likely that the great benefits potentially deriving from big data can only be achieved at the expense of individual and collective identity, i.e., the "identity paradox". Thirdly, while big data is welcomed as a tool to transform society, its tendency to concentrate power in the hands of few governments and large companies, to the detriment of individuals, should not be neglected. This is the "power paradox". This paradox, seen through the lenses of antitrust law,[32] is strictly linked to the interrelation between, on the one hand, data, especially when personal data, which could be considered "the currency of the Internet" and the key to tailored services and products that satisfy consumer needs and wants; and, on the other hand, market power, which allows multi-sided platforms to extract supra-competitive amounts of personal data[33] and entrench

---

[29] Perry Rotella, "Is data the new oil?", *Forbes* (2012), https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#77bbfe6f7db3. A different perspective in Bernard Marr, "Here's why data is not the new oil", *Forbes* (2018), https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#41e9d02a3aa9. European institutions have realised the economic potential of big data and now intend to create a data economy through public-private partnerships that could make Europe a leader in the global market (https://ec.europa.eu/digital-single-market/en/news/big-data-value-public-private-partnership and the Horizon 2020 strategy https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020).

[30] Louis Columbus, "Cloud computing market projected to reach $411B by 2020", *Forbes* (2017), https://www.forbes.com/sites/louiscolumbus/2017/10/18/cloud-computing-market-projected-to-reach-411b-by-2020/#6c64eb9278f2.

[31] Neil and King, "Big data ethics", 42.

[32] The expansive and revolutionary role of big data in economic markets – which antitrust seeks to oversee – has fueled "much speculation as to when and how big data should alter antitrust analysis" (Joshua Wright and Elyse Dorsey, "Antitrust analysis of big data", *Competition Law & Policy Debate* 2 (2016): 35-41, in particular 37).

[33] The privacy-antitrust interface with specific regard to big data is explored in Giuseppe Colangelo and Mariateresa Maggiolino, "Data accumulation and the privacy-antitrust inter-

their position, as well as to increasingly benefit from network effects and barriers to entry.[34]

In addition, a number of concerns surround the possible impact of big data over the rights and freedoms of individuals, especially the right to privacy and data protection. Not to be seen as incompatible with the fundamental values and rights within a society, technological advancements should take place in a way that respects fundamental rights.[35] Instead, new business models based on the commercial exploitation of big data, by making massive collection, combination, transfer and reuse of personal data for a number of purposes, trigger privacy concerns. In such a context, where the volume of data keeps growing exponentially and information is increasingly a shared resource, the protection of personal data becomes at the same time a more pressing need and a more difficult objective to achieve. Discrimination, exclusion and loss of control over data are only some of the risks that may result from the de-anonymisation of certain categories of data, from browsing activity to health data, from GPS coordinates to political beliefs.[36] Cloud computing services, however beneficial and promising for the future, are deemed to deprive users of control over data, processes and policies.[37] It follows that CSPs hosting large amounts

face: Insights from the Facebook case for the EU and the U.S.", *TTLF Working Papers*, 31 (2018): 26. This matter has been addressed in the 2016 Facebook case before the German Competition Authority (GCA), whose President, Andreas Mundt, has indeed argued that "[d]ata protection, consumer protection and the protection of competition interlink where data, as in Facebook's case, are a crucial factor for the economic dominance of a company" (Bundeskartellamt, press release of 19 December 2017, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2017/19_12_2017_Facebook.pdf?__blob=publicationFile&v=3). As explained in Colangelo and Maggiolino, "Data accumulation and the privacy-antitrust interface", in particular 4-26, the GCA has claimed that Facebook has abused its dominant position in the social networks market, by imposing bundled services (the "Facebook Package") on a take-it-or-leave-it basis. Such unfair terms and conditions were intended to accumulate ever-increasing quantities of data, both "on Facebook" (i.e., data generated by users' utilisation of Facebook), and "off Facebook" (i.e., data obtained from third-party sites, either external or owned by Facebook itself – like Instagram and WhatsApp).

[34] For a thorough analysis on platform market power see Kenneth Bamberger and Orly Lobel, "Platform market power", *Berkeley Technology Law Journal* 32 (2017): 1052-1092, available at SSRN: https://ssrn.com/abstract=3074717.

[35] European Data Protection Supervisor (EDPS), "Meeting the challenges of big data".

[36] European Commission, *The EU data protection reform and big data factsheet*, 2016, http://ec.europa.eu/justice/data-protection/files/data-protection-bi g-data_factsheet_web_en.pdf.

[37] Siani Pearson, "Privacy, security and trust in cloud computing", in *Privacy and Security for Cloud Computing, Computer Communications and Networks*, ed. Siani Pearson and George Yee (London: Springer, 2013), 3-42.

of data, including sensitive data, are required to implement organisational and technical measures to address any possible flaws in the protection system. Such security measures are constantly evolving, as cloud computing services are.[38] There cannot be an effective protection of users' privacy without proper efforts to continuously guarantee security and resilience.

3. Security and resilience: the real challenges for cloud service providers

In the information society,[39] where users pour their lives on the network and businesses increasingly rely on online services for their daily activities, protecting data means firstly to ensure their security throughout their value cycle. Data security in turn involves guaranteeing an adequate degree of protection for resources, achieved through the implementation of a comprehensive procedure based on a continuous cycle of assessment and re-evaluation of risks and the consequent implementation of adequate organisational and technical measures that ensure persistent data protection. This entails, on the one hand, the maintenance of integrity, confidentiality and availability of data – regardless of the means whereby data is stored, processed or transmitted – and, on the other hand, effectively counteracting any threat, whether internal or external, accidental or intentional.

In other words, security is not just an end result, but a *process*, which requires constant and simultaneous compliance with the three following requirements (also known with the acronym CIA): (i) confidentiality, i.e., protection against unauthorised access and disclosure; (ii) integrity, i.e., protection against undue alterations and deletions that would make the dataset inaccurate and unreliable; and (iii) availability, i.e., users' possibility to access and use the data upon request and with adequate response time.

Since the dawn of the Internet, compliance with these requirements has been endangered by the initiatives of hackers or crackers, who intend to exploit system vulnerabilities in software, hardware or process, and to cause the destruction of resources and the creation of damages for users.[40]

---

[38] Gholami and Laure, "Big data security and privacy issues", 59 and 66.

[39] The concept of "information society" was theorised for the first time by Daniel Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting* (New York: Basic Books, 1973). For an overview of the interpretations and theories related to this concept, please refer to Frank Webster, *Theories of the Information Society* (New York: Routledge, 2014).

[40] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 37 and 60.

In order to obtain personal information – to be sold, for instance, on the black market – cybercriminals constantly look for vulnerabilities and adapt their tactics to cope with new security measures. The incidence and severity of cyber threats is increasing: for instance, a new specimen of malware seems to be developed every second. The companies most at risk of being breached are those dealing with personally identifiable information (PII), together with payment card industry information (PCI) and protected health information (PHI).[41]

Besides, cloud storage – as any other digital environment – is vulnerable to "traditional" threats, such as malware, denial of services and ransomwares, even in the most recent version of crypto-ransomware. Given the unique technological architecture of the cloud, as well as its operating models, further risks emerge at the following levels: plants (physical security), infrastructure network (network security), information systems (system security) and applications (application security).

Cloud-related risks have been mapped by the European Network and Information Security Agency (ENISA)[42] pursuant to a risk-based approach (i.e., taking into account the probability and impact of any given threat). A distinction is possible between (i) policy and organisational risks, which may lead to, for instance, lock-in, loss of governance over security aspects, supply chain failures, and social engineering attacks; (ii) technical risks, relating, for instance, to under or over provisioning, interception of data in transit, failure to isolate data owned to different users, ineffective deletion of data, and loss of backups; and (iii) legal risks, e.g., in the event law enforcement authorities ask for the cooperation of CSPs in investigations and judicial proceedings.[43]

One of the most challenging aspects of cloud computing is the geographical dislocation of its systems. Firstly, this determines the inability to

---

[41] Minhquang N. Trang, "Compulsory corporate cyber-liability insurance: Outsourcing data privacy regulation to prevent and mitigate data breaches", *The Minnesota Journal of Law, Science & Technology* 18 (2017): 389-425, in particular 395.

[42] European Union Agency for Network and Information Security (ENISA) was established in 2004 pursuant to Regulation (EC) No. 460/20048 with the purpose of contributing to the goals of ensuring a high level of network and information security within the Union, and of developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. See further at https://www.enisa.europa.eu e https://europa.eu/european-union/about-eu/agencies/enisa_it.

[43] ENISA, "Cloud computing. Benefits, risks and recommendations for information security" (2012): 17-26, https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.

identify the exact location of data at any given time. Although this may be of little concern for users in the context of the normal use of cloud services, it becomes particularly important in the event of security breaches, when the recovery of data is dependent on the localisation of the data. Secondly, the location of the data is a fundamental criterion for determining the applicable law. Data stored in data centers located in multiple jurisdictions may trigger the applicability of multiple national laws – which may not always be perfectly compatible. [44]

Against this backdrop, security – as described above in terms of integrity, confidentiality and availability – should be pursued through organisational and technical measures, holistically and throughout the data value cycle, i.e., the phases through which data is transformed to finally lead to innovation: (i) datification and data collection, which occurs by digitalisation and by monitoring even (offline) world activities through sensors; (ii) the creation of big data, i.e., a large pool of data with no inherent meaning or structure until processed via data analytics; (iii) data analytics, intended as a set of techniques, software and skills aimed at extracting information from data; (iv) the creation of a knowledge base; and (v) data-driven decision making.[45]

Similarly, security shall be pursued at every stage of the product lifecycle – from development to usage until end-life – insofar as such products entail the collection and generation of data. This is particularly relevant in relation to the Internet of Things (e.g., smart home devices,[46] remote medical care tools for smart hospitals,[47] smart cars,[48] and Intelligent Public

---

[44] Alberto Manfredi, Francesca Capuano and Matteo Mangini, "La gestione del rischio nel cloud computing: Quali approcci e strumenti appropriati", *ICT Security*, 2016, http://cloudsecurityalliance.it/wp-content/uploads/2012/12/Rub.-Manfredi-NIS.pdf.

[45] OECD, "Data-driven innovation for growth and well-being. Interim synthesis report", *OECD Publishing* (2014), https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf: 23, where it is specified that "data-driven innovation is not a linear process, and thus cannot be sufficiently represented through a simple value chain. In contrast, data-driven innovation involves feed-back loops at several phases of the value creation process".

[46] ENISA, *Security and Resilience of Smart Home Environments. Good Practices and Recommendations* (2015), https://www.enisa.europa.eu/publications/security-resilience-good-practices.

[47] ENISA, *Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures* (2016), https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals.

[48] ENISA, *Cyber Security and Resilience of Smart Cars. Good Practices and Recommendations* (2017), https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

Transport systems[49]). But great efforts have also been dedicated to cloud computing, with ENISA launching the Cloud Security and Resilience Expert Group in 2013 and issuing a number of reports on the matter.[50]

At the organisational level, governance obligations include the implementation of security policies and procedures, proper training and management of personnel, periodic risk assessments and regular audit programmes. Technical measures should be implemented to address each security issue – namely integrity of the devices collecting data, source validation, infrastructure security, secure data management, platform and application software security, supply chain security, and interoperability of applications – through access control and authentication, encryption, source filtering, monitoring and logging, security testing procedures and audits, as well as compliance with standards and certification mechanisms.[51]

Overall, it has been observed that "because of the constant innovations that characterize the digital sector and to respond to them in an appropriate manner, any cyber security strategy must be accompanied by a foresight exercise intended to anticipate emerging technological, cultural and criminal trends."[52] However, despite numerous and sophisticated measures, the total elimination of risks connected to big data and cloud computing is difficult to achieve as "no data is totally safe".[53]

In such a complex scenario where security cannot be guaranteed yet must be pursued – thereby becoming one of the most critical factors for any CSP – it is the concept of *resilience* to digital thread that proved the means to guaranteeing a safe ecosystem.

---

[49] ENISA, *Cyber Security and Resilience of Intelligent Public Transport. Good Practices and Recommendations* (2016), https://www.enisa.europa.eu/publications/good-practices-recommendations.

[50] The following reports have been delivered in the last years: "Good practice guide for securely deploying governmental clouds"; "Incident reporting for cloud computing; critical cloud computing; cloud standards, a preliminary report" (2014); "Cloud computing risks" (2012). Please find the complete list and the relevant documents at https://resilience.enisa.europa.eu/cloud-security-and-resilience.

[51] Jasmien César and Julien Debussche, "Novel EU legal requirements in big data security. Big data – big security headaches?", *Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (2017): 83. On this also Cesare Gallotti, *Sicurezza delle Informazioni. Analisi e Gestione del Rischio* (Milan: Franco Angeli Edizioni, 2003): 101-196.

[52] Benoit Dupont, "The cyber security environment", 3.

[53] Giuseppe Saccardi, "Cyber security e resilienza: come gestire il rischio", *Tom's Hardware*, 2016, https://www.tomshw.it/cyber-security-resilienza-come-gestire-rischio-74808.

Resilience, a notion arising from the convergence of the notions of cyber security and business continuity, is "the ability of an organization to anticipate, prepare, respond and adapt actively to events, whether they are gradual or sudden changes, so as to ensure their survival".[54] A CSP, therefore, after adequately respecting the four pillars on which each cyber-resilience structure is based,[55] must be able to promptly deal with any cyber-attacks proactively, dynamically and efficiently, to safeguard the integrity, confidentiality and availability of data, as well as to ensure satisfactory levels of Objective Recovery Point, Recovery Time Objective and Recovery Capacity Objective,[56] and, more generally, promptly restore the status quo prior to accident, possibly adopting alternative modes of operation for the future. On the other hand, as there is no single definition, path, or strategy for resilience, there is the risk that it becomes just an empty word inserted into organizational planning documents. Whereas, like all the other cybersecurity solutions, resilience is not just a matter of architecture and organization, rather a matter of people and processes."[57]

4. Security obligations under the NIS Directive, the GDPR and the Proposed Cybersecurity Act

As any other technological advancements, the development of big data and cloud computing has largely occurred in a regulatory vacuum. This has

---

[54] *Ibid*. Similarly, the BS 65000 standard refers to "organisational resilience" as: "the ability to anticipate, prepare for, respond and adapt to events – both sudden shocks and gradual change. That means being adaptable, competitive, agile and robust". BS 65000, *Guidance for Organizational Resilience*, The British Standards Institution, 2014, 1.

[55] According to the National Association of Risk Managers and Corporate Insurance Managers (ANRA), the four pillars of a cyber-resilience strategy are: (1) preparation, i.e., identifying the fundamental assets of the company, and protecting them depending on the different levels of risk, so as to integrate risk management into the company structure; (2) protection, which includes staff education and training, audits and the implementation of appropriate crisis handling procedures; (3) analysis, i.e., continuous monitoring of malfunctioning and threats; (4) development, by keeping a database of incidents. ANRA, *Adattarsi al cambiamento: la resilienza alle minacce digitali*, 22 February 2016, http://www.anra.it/portal/contenuti/operativi/944/adattarsi-al-cambiamento-la-resilienza-alle-minacce-digitali.

[56] Recovery Point Objective (RPO) is the maximum amount of data lost due to a disaster that a process can tolerate, while Recovery Time Objective (RTO) measures the time period within which a process of business must be restored after the incident, and Recovery Capacity Objective (RCO) quantifies the minimum resources needed to restore operations. Alberto Manfredi, Francesca Capuano and Matteo Mangini, "La gestione del rischio", 23.

[57] Singer and Friedman, "Cybersecurity and cyberwar", 173.

been initially the case even within the European Union, where, though, over time multiple security requirements have been introduced by different European pieces of legislation sharing a common goal: the creation of a secure, trustworthy and thriving Digital Single Market.[58]

While the EIDAS Regulation imposed security obligations in relation to electronic identification means and trust services only,[59] it is in 2016 that the European legislator addresses information and network security through broader-in-scope legal instruments: the GDPR to protect the security of personal data as strictly related to its fair, lawful, and transparent processing and its free movement,[60] and the NIS Directive to promote a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.[61]

CSPs and any big data service providers should duly take into account the significant symmetries of the GDPR and the NIS Directive, which – among other things – share a similar definition of network and information security, as the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, those network and information systems.[62] Similarly, these two pieces of legislation deem security to be essential to the achievement of their goals, which include the creation of trust and confidence, the establishment of a trustworthy level playing field and the development of the internal market.[63]

---

[58] As stated by the European Commission, "[t]he Digital Single Market strategy aims to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy". Further information can be found at https://ec.europa.eu/digital-single-market/en.

[59] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, 73-114, Article 1, paragraph 1.

[60] GDPR, Article 1, and 5; Recitals 2, 13, 39, and 83.

[61] NIS Directive, Article 1, paragraph 1.

[62] GDPR, Recital 49; NIS Directive, article 4, paragraph 2.

[63] GDPR, Recital 7; NIS Directive 31 and 44.

However, while the GDPR applies to the extent that CSPs host personal data,[64] either as data controllers or data processors,[65] the NIS Directive specifically includes CSPs within its scope of application as "providers of digital services", together with online marketplaces and online search engines.[66] In addition, the latter leaves to digital services providers to self-assess whether they are targeted by the online security obligations set by the directive, which, in contrast, are mandatory for providers of "essential services", i.e. providers which are typically engaged in sectors such as energy, transport, banking, stock exchange, healthcare, utilities, and digital infrastructure.[67] Similarly, big data service providers may fall within the scope of the GDPR and the NIS Directive depending on the nature of data processed, the type of service provided, and the sector they operate.

Beside any transposing national laws,[68] providers should adopt "appropriate", "adequate" and "proportionate" measures, both organizational and technical in nature, on the basis of a culture of risk management, involving risk assessment and the implementation of security measures commensurate with the degree of risk.[69] In addition, "the state of the art

---

[64] Pursuant to GDPR, Article 4, no. 1, "'personal data' means 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."

[65] According to the definitions provided under Article 4, no. 7 and 8, "'controller' means 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", while "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

[66] This is specified in Annex III, which lists those providing a "digital service" for the purposes of Article 4, paragraph 5, i.e., any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

[67] For the purposes of Article 5 of the NIS Directive an "essential service" is identified on the basis of three criteria: "(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service". A list detailing which services qualify must be prepared (and periodically reviewed) by each Member State, also on the basis of the services described in Annex II.

[68] The GDRP is a regulation, so, by definition, directly applicable through the European Union territory; however, some discretion is left to Member States with regard to certain aspects. In contrast, the NIS Directive must be transposed by Member States into their national law; for instance, in Italy through the Legislative Decree no. 65 of 18 May 2018, OJ General Series no. 132 of 9 June 2018.

[69] According to the NIS Directive, "'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems" (Article

and the costs of implementation, as well as the nature, scope, context and purposes of processing" are crucial in determining the level of security adequate to minimise the risk.[70] Accordingly, effective measures may include pseudonymisation and encryption of personal data,[71] accurate selection of third-parties providers to which processing is outsourced,[72] as well as regular testing, assessing and evaluating the effectiveness of technical and organisational measures,[73] to be updated in case of changed circumstances.[74]

Moreover, procedures should be introduced by each provider to ensure effective incident handling and resilience of network and information systems,[75] but also compliance with the notification requirements prescribed by law in the event of security incidents that endanger the continuity or provision of essential services or digital services,[76] and in case of breach of personal data.[77]

The accountability principle should inspire any CSPs,[78] which should also follow best practices[79] and all decisions, guidelines or instructions of the relevant authorities, namely: pursuant to the GDPR the European Data Protection Supervisor, the supervisory authorities established by Member States, and the European Data Protection Board;[80] and according to the NIS Directive the European Union Agency for Network and Information

---

4, no. 9) and "risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact" (Recital 46). See also article 7, 14 and 16 of the NIS Directive. A risk-based approach to security is also common to the GDPR, Recitals 75-77 and Articles 5, 24 and 32. According to the latter, risk is parametered to "varying likelihood and severity for the rights and freedoms of natural persons".

[70] GDPR, Articles 25 and 32. Similarly, NIS Directive, Articles 14 and 16.

[71] GDPR, Article 32, paragraph 1, letter a).

[72] GDPR, Article 28.

[73] GDPR, Article 32, paragraph 1, letter d).

[74] GDPR, Article 24, paragraph 1.

[75] An internal security strategy should be shaped on the basis of the incident lifecycle: pre-incident, where measures to detect, contain and respond to risks should be constantly reviewed and adapted; during the incident, where technical, legal, management, reputational and financial experts should work together to handle the incident; and post-incident, where evidence of security measures, policy and procedures, incident response plan and risk mitigation plans, investigations and disciplinary actions play a fundamental role. For more details, César and Debussche, "Novel EU legal requirements", 86-87.

[76] NIS Directive, Article 8, 14 and 16.

[77] GDPR, Recitals 85 and 86, Articles 33 and 34.

[78] GDPR, Recital 85 and Article 5, paragraph 2.

[79] GDPR, Recital 77, Article 70; NIS Directive, Recitals 35-36 and Article 11.

[80] GDPR, Section 3.

Security (ENISA), the national competent authorities (NCAs),[81] the computer-security incident response teams (CSIRTs),[82] the cooperation group and the CSIRT network comprising representatives of EU countries' CSIRTS and the Computer Emergency Response Team (CERT-EU).

This mix of hard and soft law that providers are supposed to follow is the result of the variety and complexity of existing technologies, which, combined with the rapid pace of their evolution, make it impracticable for the legislator to specify in detail the necessary technical measures to implement in any given case. Beside pieces of legislation such as the GDPR and the NIS directive, codes of conduct, certification mechanisms and standards elaborated by private subjects are not only strongly encouraged but also needed.[83]

In addition to the instruments above, and as part of the so-called "Cybersecurity package",[84] the European Commission has adopted a new proposal for a Cybersecurity Act so as to establish "a high level of cybersecurity, cyber resilience and trust within the Union with a view to ensuring the proper functioning of the internal market".[85] The proposed Regulation defines cybersecurity as encompassing "all activities necessary to protect network and information systems, their users, and affected persons from cyber threats"[86] and it aims at (i) strengthening the role of ENISA – which should act as a reference point of advice and expertise on cybersecurity for Union institutions, agencies and bodies,[87] and (ii) establishing a European cybersecurity certification framework for ICT products and services. This is based on the awareness that "network and information systems and telecommunications networks and services play a vital role for society and have become the backbone of economic growth;[88] yet, at the same time, increased digitisation and connectivity generate an higher number of

[81] NIS Directive, Article 8.

[82] NIS Directive, Article 9.

[83] GDPR, article 24, paragraph 3, 28, paragraph 5, 32, 40 and 42. E.g., the ISO/IEC 27000 series issued by the International Standards Organisation (the ISO) and the International Electrotechnical Commission (the IEC).

[84] The progress made by the European Commission with regard to this initiative can be monitored at https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en.

[85] Cybersecurity Act, Article 1.

[86] *Ibid.*, Article 2.

[87] *Ibid.*, Article 3.

[88] *Ibid.*, Recitals 1 and 3.

cybersecurity risks, which in turn make society at large more vulnerable to cyber threats and exacerbate dangers faced by individuals.[89]

5. Contractual shields to providers' liability

When devising and launching technologically every day more sophisticated products and services, providers find themselves confronted with progressively more complex risks. Under a legal perspective, these risks translate into terms of responsibility. Accordingly, a business should implement a thoughtful information security following at least a twofold reason: protecting corporate assets (including those having a strategic relevance, such as intellectual property and new product information) and business reputation, which could be harmed by the adverse publicity caused by a security breach; and establishing diligence by documenting reasonable corporate management and minimising potential liability.[90] In fact, given that companies are now dependent on data and information technology for carrying their businesses' operations, cybercrimes causing their data to be lost or distorted may determine business interruptions, the inability to meet contractual obligations with counterparties, and the risk of both class action lawsuits being filed by individuals damaged by the data breach, and derivative lawsuits filed by the company's shareholders against the board of directors. In addition, cybercriminals could use extort companies or trade on insider information.[91] These liability risks turn into burdensome costs; indeed, data security breaches are deemed to possibly account for over $400 billion in losses annually.[92]

This is even truer in the case of data breaches as the safe harbour set by Article 14 of the E-Commerce Directive[93] does not cover big data and cloud service providers with regard to security obligations. The above safe harbour applies to cloud service providers and exempts them – and more in general any hosting providers – from liability as long as the information

---

[89] *Ibid.*

[90] James R. Kalyvas and Michael R. Overly, *Big Data. A Business and Legal Guide* (London: CRC Press, 2015), 15.

[91] Minhquang N. Trang, "Compulsory corporate cyber-liability insurance", 390-391 and, for a detailed account of some notable lawsuits, 398-405.

[92] PwC, "Insurance 2020 & beyond: Reaping the dividends of cyber resilience", 2015, https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf: 4.

[93] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), OJ L 178, 17.7.2000, 1-16.

is stored at the request of a recipient of the service and they have not actual knowledge of, or control over, the data processed, stored or transmitted upon request of users that are illegal (e.g., in contrast with intellectual property law, defamatory content, hate speech, etc. Therefore, with regard to big data and cloud service providers' security obligations, it remains their primary responsibility to ensure data confidentiality, integrity and availability, as well as resilience. And no exemption is at the moment envisaged in the current legal framework.

In light of this, besides internally applying mitigation measures, companies include security-related safeguards in contracts entered into with either business partners or customers, including confidentiality clauses, detailed security obligations, warranties, indemnity provisions, audit rights, and limitations of liability. In fact, entrusting big data to a business partner always requires a careful due diligence activity and adequately reflecting any resulting issue in the agreement between the parties. Outsourcing certain activities to third parties may be risky and related security risks are partly mitigated through due diligence, contractual protections and an information security requirements exhibit.[94]

This is why, with specific regard to CSPs, Service Level Agreements (SLAs) – which constitute, together with the Terms of Service (ToS), a fundamental part of cloud contracts – are particularly relevant. SLAs detail the qualitative and quantitative standards of the service, also in relation to service availability and reliability, authentication systems, encryption mechanisms, monitoring and periodic audits, and incident handling.[95] Through SLAs, CSPs voluntarily assume, on a negotiation basis, the obligation to guarantee adequate standards of security in the provision of their services, with the ultimate goal of inspiring trust among users and strengthening a reputation as reliable market operators. In this way, any breach becomes a matter of contractual liability as well. SLAs are often made available in the CSPs' websites, which can be amended by the latter,

---

[94] For more details about this see Michael R. Overly, "Information security in vendor and business partner relationships", in *Big Data. A Business and Legal Guide*, ed. James R. Kalyvas and Michael R. Overly (London: CRC Press, 2015), 21-31.

[95] Typically, SLAs address (i) service performance – in terms of availability, response times, capacity parameters, etc. – and assistance service; (ii) data management, including backup and portability procedures; and (iii) data protection, in accordance with the requirement of the applicable law. On this Shyam S. Wagle, "Cloud computing contracts. Regulatory issues and cloud providers' offer: An analysis", IFIP, 2016, http://www.ifip-summerschool.org/wp-content/uploads/2016/08/IFIP-SC-2016_pre_paper_11.pdf: 6.

leaving generally to users the onus to monitor any change. In addition, remedies for breach usually consist in service credits.[96] In addition, when personal data are involved, a data processing agreement is also to be entered into by the parties, pursuant to article 28 of the GDPR, to provide "sufficient guarantees" that the requirements of the GDPR will be met and the rights of data subjects protected.

It has however been observed that despite the agreements above CSPs do not always provide clear and complete security-related information, especially in the context of contractual relations with consumers.[97] From a compared analysis of the terms and conditions adopted by the main CSPs, many critical aspects emerge,[98] which may derive from the unequal bargaining force of the parties. In fact, cloud contracts are often considered a "take it or leave it" option unilaterally set by CSPs, which are hardly inclined to change their standard terms[99] on the assumption that "in trying to remove or reduce liability exclusions and limitations or increase service levels for commoditized services, customers want to have their cake and eat it too – seeking the cheapest services while requesting the highest levels of assurances."[100] At the same time, negotiating terms could not be advisable for a pragmatic reason: compliance with all users' separate security policies – which may impose different, even conflicting, requirements – is deemed to be difficult in a standardised infrastructure.[101]

Other recurrent – and problematic – clauses relate to the limitation of CSPs' liability and advance liquidation of damage in the event of any breach of the security obligations on CSPs,[102] which makes contractual

---

[96] W. Kuan Hon, Christopher Millard, and Ian Walden, "Negotiating cloud contracts: Looking at clouds from both sides now", *Stanford Technology Law Review* 16 (2012): 79-129, in particular 98.

[97] Frank Alleweldt *et al.*, "Cloud computing", *Studio del Parlamento Europeo-Direzione generale politiche interne*, 2012, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_IT.pdf: 59-67.

[98] E.g., the disproportion between the rights and obligations of the parties, including the right of the CSP to suspend the service or unilaterally change the terms of the service. Simon Bradshaw, Christopher Millard and Ian Walden, "Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services", *Queen Mary School of Law Legal Studies* 63 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.

[99] These contracts are often configured as click wrap agreements, i.e. contracts in which the negotiated consent is reduced to a check in the "Accept" box at the bottom of the screen. They are negotiated rarely, when the client has a significant bargaining power.

[100] Hon, Millard, and Walden, "Negotiating cloud contracts", 95.

[101] Hon, Millard, and Walden, "Negotiating cloud contracts", 112.

[102] Hon, Millard, and Walden, "Negotiating cloud contracts", 79-129.

protections largely illusory.[103] In bold and capital letters, it is often clarified that services are offered "as is" and "as available". The reason is well explained by, for example, Dropbox, when stating in its terms of service that they "strive to provide great Services", but there are certain things that they "can't guarantee".[104]

Consequently, although aware that disclaimers "will not apply to the extent prohibited by law",[105] a CSP typically "does not warrant uninterrupted or error-free operation of a Cloud Service or that IBM will correct all defects or prevent third party disruptions or unauthorized third party access".[106] In addition, not only no warranty is given that "the operation of the software or the services will be error-free or uninterrupted", but "any other warranty of any kind, whether express, implied, statutory or otherwise, including warranties of merchantability, fitness for a particular use and no infringement" is excluded "to the maximum extent permitted by applicable law".[107]

Accordingly, pursuant to CSPs' general conditions, no damages – may that be direct, indirect, incidental, special, consequential, punitive or exemplary – can be claimed for, among other things, "unscheduled downtime of all or a portion of the services" or "any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of your content or other data".[108]

Although many providers take multiple backups of data, they will not commit contractually to doing so, nor warrant data integrity or accept

---

[103] Overly, "Information security", 29. Such limitations are of doubtful compatibility with European legislation on unfair terms in consumer contracts. Pursuant to Directive 93/13/EEC of April 5, 1993, Annex Clause referred to in Article 3, paragraph 3, letter q., are considered to be abusive, *inter alia*, the clauses which "improperly exclude or limit the legal rights of the consumer towards the professional or another party in the event of total or partial non-performance or defective performance by the professional any contractual obligation, as well as those which have as their object or effect the suppress or limit the exercise of legal actions or remedies by the consumer".

[104] Dropbox, "Terms of service", https://www.dropbox.com/privacy?view_en#terms.

[105] SalesForce, "Master subscription agreement", paragraph 11(2), https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/salesforce_MSA.pdf.

[106] IBM, "Cloud services agreement", paragraph 4(b), https://www.ibm.com/support/customer/pdf/csa_us.pdf.

[107] Google, "Google cloud platform terms of service", paragraph 12, https://cloud.google.com/terms/.

[108] Amazon, "AWS customer agreement", paragraph 11, https://aws.amazon.com/it/agreement/.

liability for any data loss.[109] It is also stressed that security is a shared responsibility with users.[110]

Moreover, most of the times, in the event that a CSP actually incurs liability, a threshold is introduced by contract, which typically states that "the maximum, aggregate liability to the other under this agreement is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the applicable Products during the term of this agreement", and similarly SAP and Aruba[111].

Thus, while investing in security, as an essential condition to establish themselves as reliable and competitive market operators – and while involved in (or dragged into) initiatives aimed at developing adequate safety standards, codes of conducts and certifications – in their daily business activities CSPs use contract law to escape – to the maximum extent allowed by law – any liability that may arise from security breaches, which would be a great cost also in terms of adverse publicity. The significant bargaining power most CSPs enjoy allows them to impose their contractual terms upon customers and business partners that lack equal strength.

In other words, one the one hand, CSPs help in addressing the existent "jungle of standards"[112], also cooperating with the European

---

[109] Hon, Millard, and Walden, "Negotiating Cloud contracts", 96.

[110] Amazon, "Amazon web services: Overview of security processes", 2017, 1-93. https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

[111] Microsoft, "Cloud agreement", paragraph 7, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiS-4nuj_7bAhWpCpoKHaEfCekQFghFMAE&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F2%2FC%2F8%2F2C8CAC17-FCE7-4F51-9556-4D77C7022DF5%2FMCA2016Agr(Asia)JPN(ENG)(Jul2016)(CR).pdf&usg=AOvVaw2DhYg5SzpxKW-YDTNvBdcf). Similarly, another example is Aruba, which "shall be liable solely for an amount equal to the sum spent by the Customer over the last 12 months". SAP, "General terms and conditions for SAP Cloud Services", paragraph 9(2), https://www.sap.com/about/cloud-trust-center/cloud-service-level-agreements/cloud-services.html?search=General%20Terms%20and%20Conditions&sort=title_asc#pdf-asset=8c3d65cc-e67c-0010-82c7-eda71af511fa&page=5: "the maximum aggregate liability of either party (or its respective Affiliates or SAP's subcontractors) to the other or any other person or entity for all events (or series of connected events) arising in any twelve month period will not exceed the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve month period". Aruba, "Terms and conditions for the provision of the Aruba Cloud Service", paragraph 7(2) and 8(1), https://www.arubacloud.com/documents/tc-files/en/1_termsandconditionsprovisionarubacloud.pdf: "Aruba […] shall be liable solely for an amount equal to the sum spent by the Customer over the last 12 months".

[112] In September 2012, the European Commission described cloud computing as a fundamental tool for progress for citizens, businesses and public institutions, as well as for the whole of Europe; at the same time, it identified a "jungle of standards" as the main obstacle to the affirmation of cloud com-

Commission;[113] on the other hand, they use cloud contracts as a shield from liability.

From a different perspective, mindful of the ever-evolving nature of cyber threats, CSPs and, more generally, companies can recur to cyber-liability insurance to outsource the risks relating to cybersecurity compliance to the insurance industry. A step further in this direction could be taken by governments themselves by making cyber-liability insurance compulsory – at least for companies meeting certain requirements. This would shift the obligation to determine compliance requirements from the legislator – whose action is generally influenced by the political climate – to insurance companies – which are best placed to deal with highly technical and rapidly changing issues. Insurers would have a monetary incentive to adopt state-of-the-art and effective cybersecurity standards and this would lead not only to the minimisation of risks, but also to the mitigation of damages. In other words, both companies at risk and the public at large would benefit from the implementation of a compulsory cyber-insurance scheme.[114]

Bibliography

Alleweldt, Frank, Senda Kara, Anna Fielder and Ian Brown."Cloud computing". *Studio del Parlamento Europeo – Direzione generale politiche interne* (Bruxelles: European Parliament, 2012), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_IT.pdf.

ANRA.*Adattarsialcambiamento:laresilienzaalleminaccedigitali*.22February2016,http://www.anra.it/portal/contenuti/operativi/944/adattarsi-al-cambiamento-la-resilienza-alle-minacce-digitali.

Armerding, Taylor. "The 17 biggest data breaches of the 21st century. Security practitioners weigh in on the 17 worst data breaches in recent memory". *CSO*. January 26, 2018. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

puting and therefore as a barrier to economic development. European Commission, "Unleashing the potential of cloud computing in Europe", COM (2012) 529 final, 27 September 2012.

[113] For an interesting overview and analysis of the initiatives undertaken by the European Commission, as well as numerous public and private organisations, in the field of cloud computing and standard processing, please refer to Niamh Christina Gleeson and Ian Walden, "'It's a jungle out there'? Cloud computing, standards and the law", *European Journal of Law and Technology* [Online] 5, no. 2 (2014), http://ejlt.org/article/view/363/460.

[114] Minhquang N. Trang, "Compulsory corporate cyber-liability insurance", 409.

Badger, Lee, Tim Grance, Robert Patt-Corner and Jeff Voas. *Cloud Computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology (2012).

Barocas, Solon, Sophie Hood, and Malte Ziewitz. "Governing algorithms: A provocation piece". March 29, 2013. http://governingalgorithms.org/resources/provocation-piece/.

Barrett, Meredith A., Olivier Humblet, Robert A. Hiatt and Nancy E. Adler. "Big data and disease prevention: From quantified self to quantified communities". *Big Data* 1 (2013): 168-175.

Bell, Daniel. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Reissue. New York: Basic Books, 1973.

Bench-Capon, Trevor *et al*. "A history of AI and Law in 50 papers: 25 years of the international conference on AI and Law". *Artificial Intelligence and Law* 20 (2012): 215-319.

Berry, Michael J. and Gordon S. Linoff. *Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management*. New Jersey: John Wiley & Sons, 2004.

Boyd, Danah and Kate Crawford. "Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon". *Information, Communication & Society* 15 (2012): 662-679.

Bradshaw, Simon, Christopher Millard and Ian Walden. "Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services". *Queen Mary School of Law Legal Studies*, 63 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.

César, Jasmien and Julien Debussche. "Novel EU legal requirements in big data security. Big data – big security headaches?". *Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (2017): 79-88.

Cisco. "Visual networking index: Global mobile data traffic forecast update 2016-2021". 28 March 2017, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

Colangelo, Giuseppe and Mariateresa Maggiolino, "Data accumulation and the privacy-antitrust interface: Insights from the Facebook case for the EU and the U.S.", *TTLF Working Papers*, 31 (2018): 2-46.

Columbus, Louis. "Cloud computing market projected to reach $411B by 2020". *Forbes*. October 18, 2017. https://www.forbes.com/sites/louiscolumbus/2017/10/18/cloud-computing-market-projected-to-reach-411b-by-2020/#6c64eb9278f2.

Cook, James. "FBI director: China has hacked every big US company". *Business Insider*. October 6, 2014. http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10?IR=T.

De Filippi, Primavera. "Big data, big responsibilities". *Internet Policy Review* 3 (2014): 1-12.

Dupont, Benoit. "The cyber security environment to 2022: Trends, drivers and implications", 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208548.

ENISA. "Cloud computing. Benefits, risks and recommendations for information security", 2012. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.

ENISA. "Cyber security and resilience of intelligent public transport. Good practices and recommendations", 2016. https://www.enisa.europa.eu/publications/good-practices-recommendations.

ENISA. "Cyber security and resilience of smart cars. Good practices and recommendations", 2017. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

ENISA. "Security and resilience of smart home environments. Good practices and recommendations", 2015. https://www.enisa.europa.eu/publications/security-resilience-good-practices.

ENISA. "Smart hospitals. Security and resilience for smart health service and infrastructures", 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals.

European Commission. "The EU data protection reform and big data factsheet", 2016. http://ec.europa.eu/justice/data-protection/files/data-protection-bi g-data_factsheet_web_en.pdf.

European Commission. "Unleashing the potential of cloud computing in Europe". COM (2012) 529 final, 27 September 2012.

European Data Protection Supervisor (EDPS). "Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability". Opinion 7/2015, 19 November 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

Evans, Dave. "How the Internet of Everything will change the world ... for the better #IoE". November 7, 2012. https://blogs.cisco.com/digital/how-the-internet-of-everything-will-change-the-worldfor-the-better-infographic.

Franks, Bill. *Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics*. New Jersey: John Wiley & Sons, 2012.

Gallotti, Cesare. *Sicurezza delle Informazioni. Analisi e Gestione del Rischio*. Milan: Franco Angeli Edizioni, 2003.

Gantz, John and David Reinsel. "Extracting value from chaos". *International Data Corporation*. June 2011. https://uk.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf.

Gholami, Ali and Erwin Laure. "Big data security and privacy issues in the cloud". *International Journal of Network Security & its Applications* 8 (2015): 59-79.

Gleeson, Niamh Christina and Ian Walden. "'It's a jungle out there'? Cloud computing, standards and the law". *European Journal of Law and Technology* [Online] 5, no. 2 (2014). http://ejlt.org/article/view/363/460.

Hon, W. Kuan, Christopher Millard and Ian Walden. "Negotiating cloud contracts: Looking at clouds from both sides now". *Stanford Technology Law Review* 16 (2012): 79-129.

Kalyvas, James R. and Michael R. Overly. "Big data. A business and legal guide". London: CRC Press, 2015.

Kranzberg, Melvin. "Technology and history: Kranzberg's laws". *Technology and Culture* 27 (1986): 544-560.

Lazar, Nicole. "The big picture: Big data hits the big time". *Chance* 25 (2012): 47-49.

Manfredi, Alberto, Francesca Capuano and Matteo Mangini. "La gestione del rischio nel cloud computing: quali approcci e strumenti appropriati". *ICT Security*. July / August 2016. http://cloudsecurityalliance.it/wp-content/uploads/2012/12/Rub.-Manfredi-NIS.pdf.

Marr, Bernard. "Here's why data is not the new oil". *Forbes*. March 5, 2018, https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#41e9d02a3aa9.

Mayer-Schonberger, Viktor and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. New York: Houghton Mifflin Harcourt, 2013.

Neil, Richards and Jonathan King. "Big data ethics". *Wake Forest Law Review* 49 (2014): 393-432.

OECD. "Data-driven innovation for growth and well-being. Interim synthesis report". *OECD Publishing*, 2014. https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf.

Pearson, Siani. "Privacy, security and trust in cloud computing". In *Privacy and Security for Cloud Computing, Computer Communications and Networks*, edited by Siani Pearson, George Yee, 3-42. London: Springer, 2013.

PwC. "Insurance 2020 & beyond: Reaping the dividends of cyber resilience". 2015. https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

Richards, Neil M. and Jonathan H. King. "Three paradoxes of big data". *Stanford Law Review online* 66 (2013): 41-46.

Rotella, Perry. "Is data the new oil?". *Forbes*. April 2, 2012. https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#77bbfe6f7db3.

Saccardi, Giuseppe. "Cyber security e resilienza: come gestire il rischio". *Tom's Hardware*. March 4, 2016. https://www.tomshw.it/cyber-security-resilienza-come-gestire-rischio-74808.

Schoutem, Edwin. "Cloud computing defined: Characteristics & service levels". *IBM*. January 31, 2014. https://www.ibm.com/blogs/cloud-computing/2014/01/31/cloud-computing-defined-characteristics-service-levels/.

Semmler, Sean and Rose Zeeve. "Artificial intelligence: Application today and implications tomorrow". *Duke Law & Technology Review* 16 (2017): 85-99.

Singer, P. W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, Oxford University Press, 2014.

Smolan, Rick and Jennifer Erwitt. *The Human Face of Big Data*. China: Against All Odds Productions, 2012.

Steiner, Christopher. *Automate This: How Algorithms Came to Rule Our World*. London: Penguin, 2012.

Trang, Minhquang N. "Compulsory corporate cyber-liability insurance: Outsourcing data privacy regulation to prevent and mitigate data breaches". *The Minnesota Journal of Law, Science & Technology* 18 (2017): 389-425.

Wagle, Shyam S. "Cloud computing contracts. Regulatory issues and cloud providers' offer: An analysis". IFIP (2016), http://docplayer.net/42226495-Cloud-computing-contracts.html.

Webster, Frank. *Theories of the Information Society*. New York: Routledge, 2014.