Blockchain and individuals' control over personal data in European data protection law

TILBURG UNIVERSITY
Master Law & Technology

Thesis supervisor:
Prof. Lokke Moerel

Second reader:
Dr. Emre Bayamlıoğlu

Student number	Last Name	First Name	ANR
1278968	Filippone	Roberta	900639

August 2017

Table of content

Chapter I

Introduction

Blockchain is a recent technology that promises to shift control over daily activities from central parties to their users. It is seen as a means for making systems more democratic and transparent, an innovation that - through peer-to-peer architecture and cryptographic techniques - should make central intermediaries almost unnecessary and individuals more empowered. This technology paradigm pushes towards the decentralization of different areas such as business and politics, and it is deemed to have a significant disruptive impact for society at large, to the point of being described as "fundamental for forward progress in society as Magna Charta or the Rosetta Stone."[1] However, behind the promises of a higher level of individuals' freedom and control deriving from decentralization, blockchain raises several concerns. This research focuses on those issues that relate to privacy and data protection. In particular, this study means to analyse this new technology through the lens of the core of the right to data protection, namely individuals' control over their personal data, to assess whether blockchain can empower the individuals' control in compliance with European data protection law. For this reason, in this thesis I started with an overview of the main factors that have led to the individuals' loss of control over their personal data on the Internet and the need of their empowerment, the relating answers of law-regulators and techno-designers, as well as the description of blockchain technology and the reconstruction of the concept of "control." In this thesis, it is advocated that blockchain systems may not represent such an empowering technology for the protection of the individuals' right to data protection, if not specifically regulated.

1.1 The individuals' loss of control and the centralization of the Internet

The Internet was originally conceived as a distributed network of networks. The idea behind was to create an egalitarian virtual space supported by strong privacy. With this view, the internet protocol suite (TCP/IP), the end-to-end principle and cryptography were meant to allow the flow of information without any filter and, more broadly, without any central governance. This initial enthusiasm and optimism for the Internet is encapsulated in the well-known John Perry Barlow's manifesto "A Declaration of the Independence of Cyberspace" (1996), where the author proclaims the notorious words:

"*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*."[2]

However, in contrast to the original purpose, the Internet has turned into a new space for power centralization and control.[3] Intermediaries such as the Internet Service Providers play a significant role in the access to information (facilitating sometimes censorship). Besides, a few large

[1] Swan, M., (2015) "Blockchain: Blueprint for a New Economy", O'Reilly Media, p. viii.

[2] Barlow, J. P (1996) "A Declaration of the Independence of Cyberspace". Available at: https://www.eff.org/it/cyberspace-independence.

[3] Because of digital surveillance, Internet is considered a technology of control. On this point Castells, M. (2001) "The Internet Galaxy: Reflections on the Internet", Business and Society, Oxford University Press, Inc. New York, p. 171.

corporations daily dictate what we can and should read, watch, buy and who we should date, become friends with, and much more.[4] The development of social media platforms (Web 2.0)[5] has remarkably contributed to the surge of personal data shared on the Internet by its users through social networking, community building and user-generated content production. This huge quantity of data, together with lower storage costs and more sophisticated data mining techniques have increased profiling abilities of governments and commercial actors. Systematic monitoring of individuals through information technology has given rise to massive scale surveillance, also known as *dataveillance*.[6] On the one hand, users' online activity is always transparent; while, on the other hand, service providers' usage of this information is highly opaque, therefore creating a new digital form of *panopticon*.[7] More specifically, online platforms are based on a data-driven model in which personal data constitute an economic asset, the "new oil" or "new currency" of the digital world.[8] This data is pivotal for the development of digital markets and, thus, represents an important competitive element for companies also operating online.[9] Personal data has become the currency digital users pay to obtain access to online services. Indeed, this data is often provided in exchange for "free" content and/or services with a "take it or leave it" choice. Therefore, due to this business model, sharing data has become almost inevitable in the digital space. Moreover, Internet users commonly submit to terms of service agreements that they do not even read. In this way, individuals daily give license to companies to share their personal data to advertisers, governments and other institutions.

The personal data economy on which centralized platforms are based has been highly criticized in different areas, not only with regard to privacy and data protection law, but also competition and consumer law. From the privacy and data protection perspective, several concerns are raised. In particular, tracking online activities and collecting big masses of personal data at a central level make

[4] It has to be highlighted that: "*The rise of networking did not eliminate intermediaries, but rather changed who they are. It created a whole host of intermediaries, most important of which (for our purposes) are ISPs, search engines, browsers, the physical network, and financial intermediaries. In short, the Internet had made the network itself the intermediary for much conduct that we might have thought had no intermediary at all prior to the Internet*": Goldsmith, J., Wu, T. (2006) "Who Controls the Internet: Illusions of a Borderless World", 142-161, p. 70.

[5] For instance, MySpace, Youtube, Facebook, Wordpress, Twitter, LinkedIn, etc.

[6] On this point see: Clarke, R. (1994) "Dataveillance by Governments: The Technique of Computer Matching", Information Technology & People, Vol. 7 Issue: 2.

[7] The panopticon refers to an institutional building designed to better observe its inmates without them being conscious of when and how they are monitored. This model was designed in the late 18th century by the English philosopher Jeremy Bentham with regard to prisons' architecture. According to this model, prisoners in the cells are constantly aware of potential surveillance from the guards of a central tower having control of what happens in the rings of cells surrounding the tower. The panopticon theory was later developed by Michael Foucault, according to which the knowledge of being permanently visible influence our behaviours. In particular, he claims "the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power", see Foucault, M. (1977) "Discipline and punish: the birth of the prison", Pantheon Books: New York, p. 201. Digital technologies, especially the Internet, are seen as new forms of panopticons which are able to make transparent users' behaviour to the intermediary, whose behaviour on the opposite is black-boxed. On this point see also Galic, M., Timan, T., Koops, B. J. (2016) "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation", Tilburg Law School Research Paper No. 13/2016; Gordon, D. (1997) "The electronic panopticon: a case study of the development of the national crime records system", Politics and Society, 15(4): 483-511.

[8] On personal data as the "new oil": Commissioner Kuneva, Roundtable on Online Data Collection, Targeting and Profiling, 31 March 2009, http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

[9] Personal data is a fundamental asset in the platform economy because of data lock-in, improvement of products and services offered online through data analytics, better design of targeted advertisements, etc. See: Monopolkomission Report (2015) "Competition policy: The challenge of digital markets", p. 36.

it possible for businesses and governments to monitor and to reveal not only the present and the past, but even the future of individuals' habits and preferences. Through data mining techniques, central actors are able to identify common patterns within large databases and, with the help of opaque algorithms, even infer and predict future behaviours through correlation instead of causation. In this landscape, individuals whose data are being mined are often unaware of this lucrative market. Moreover, they are not put in the position to understand what the existing knowledge is about them, who has access to it, how this data is used, how they are profiled, what is the underlying logic of algorithms, and what consequences categorization and evaluation can have on their lives.[10] In such a "black-box society"[11] where individuals don't have meaningful control over their data, the risk of stigmatization, reinforcement of stereotypes, discrimination, social and cultural exclusion is of high concern. The centralization of platforms' architectures (client-server), the adoption of a data-driven business model and the fact that the web is mainly run by few large corporations have turned the World Wide Web into a highly centralized place in which privacy and users' control over their data lack. As already mentioned, this centralized evolution of the web is in total contrast with its original purpose, as the father of the World Wide Web has recently claimed.[12]

1.2 Towards more individuals' control over their personal data

The search of alternatives to the aggregation of personal data occurring in central architectures started already in the '90s and it has involved not only regulators, but also consumer advocates and software developers. In particular, in order to increase individuals' privacy and protection of personal data, law regulators - accepting some loss of individuals' control of centralized systems - have tried to reduce this loss through a more stringent regulation of data controllers; while software designers have directly aimed at eliminating any third party.

1.2.1 Regulation by Law

From the regulatory side, to cope with the challenges of the black-box society described above, on 14th April 2016 the EU Commission, Parliament and Council of Ministers agreed on the General Data Protection Regulation (GDPR), consisting of pan-European data protection rules directly applicable from 28th May 2018. This Regulation will substitute the Directive 95/46/EC, obsolete for the new technological panorama. The two main aims of the Regulation are to reinforce data protection of personal data across European member states by giving more control to individuals over their data, as well as to facilitate the free flow of personal data in the Digital Single Market. To achieve these goals, the GDPR increases the responsibilities of data controllers, introduces new principles, strengthens existing rights of individuals and introduces new ones such as the right to data portability and the right to be forgotten. The new data protection legal framework seeks to alter the relationship between data controllers and data subjects in the direction of a more balanced relationship between

[10] Gutwirth, S., et al. (2010), "Data Protection in a Profiled World", Springer: Dordrecht; See also: https://www.ft.com/content/3278e6dc-67af-11e7-9a66-93fb352ba1fe Our personal data are precious – we must take back control

[11] Pasquale, F. (2015), "The Black Box Society", Cambridge, MA: Harvard University Press.

[12] Weinberger, D., "How the Father of the World Wide Web Plans to Reclaim It from Facebook and Google", in Digital Trends, August 10, 2016, http://www.digitaltrends.com/web/ways-to-decentralize-the-web/ .

businesses and individuals when it comes to the sharing of the benefits of big data.[13] As organizations gain significant profits from the processing of customers' personal data – often without the latter being aware of it – also individuals should be put in the condition to better know how their data are used and to use them for their own purposes.[14]

1.2.2 Regulation by Technology

Apart from law regulation, another longstanding attempt to redistribute power relations over the web comes from software-designers.[15] This attempt towards "re-distribution" of the Internet started with the spread of peer-to-peer architectures, and evolved with the adoption of alternative routing systems[16] and strong advocacy of cryptography.[17] These solutions were meant to develop direct individual-to-individual interactions in order to avoid censorship and, especially after Snowden revelations in 2013 on mass surveillance programs, also digital surveillance based on third parties' control of centralized architectures. Decentralization has been advocated as the most effective way to contrast the threats of centralization and to preserve privacy and liberty as it entails the elimination of intermediaries.[18] However, for a long time decentralized systems have received only marginal adoption due to technical and economical drawbacks, such as higher network unreliability due to the

[13] EDPS - European Data Protection Supervisor (2015), Opinion 7/2015, "Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability.

[14] For instance, this direction can be seen in the introduction of the right to data portability (Art. 20 GDPR) that allows data subjects to receive and transfer their personal data from one platform to another one; as well, the European Data Protection Supervisor is strongly supporting the adoption of Personal Information Management Systems where individuals can better manage and control their online identity. See EDPS (Oct. 2016) "Opinion on Personal Information Management Systems".

[15] Techno-regulation plays a fundamental role as pointed out in: Lessig, L. (2006) "Code and Other Laws of the Cyberspace", New York: Basic Books.

[16] Dingledine, R., Mathewson, N., Syverson, P. (2004) "Tor: The second-generation onion router", 13th USENIX Security Symposium.

[17] "*We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. […] We the Cypherpunk are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money. […] Cypherpunk write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it*.", in Hughes, E. (1993) "A Cypherpunk's Manifesto", https://www.activism.net/cypherpunk/manifesto.html.

[18] youbroketheinternet. Available at: http://youbroketheinternet.org/.; Redecentralize.org. Available at: http://redecentralize.org/.

The cultural origins of strong cryptography as a means to protect privacy and freedom traces back to crypto-anarchy and cypherpunk movements; "The Crypto Anarchist Manifesto" (1988), Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html – "Cypherpunk's Manifeto" (1993). Available at: https://www.activism.net/cypherpunk/manifesto.html.

difficulties in balancing consistency and availability, the need of software installation also by inexpert users eventually resulting in a higher vulnerability of the network and more.[19]

1.3 Decentralization through blockchain

A significant evolution towards decentralization traces back to 2008, when Bitcoin technology was first theorized by Satoshi Nakamoto. Bitcoin is a decentralized payment system built upon a distributed ledger aiming at replacing some of the banks and other intermediary functions.[20] Indeed, Bitcoin's monetary supply is controlled by its protocol, without any intervention by central authorities. Bitcoin was designed to eradicate corruption from monetary management – which had its peak in the financial crises of 2008 - through a decentralized and "trustless"[21] alternative to banks and governments.[22] Bitcoin has triggered great attention, especially for the ledger technology on which it relies, namely the blockchain. As it will be described in more details in *Chapter II*, blockchain is a general-purpose technology that provides transparent and tamper-proof record of a specific state of affair on which the parties of a transaction have agreed on, without the need of a trusted third party. Blockchain entails an unprecedented process of disintermediation on a large scale which is likely to substantially impact several areas of our lives. It can potentially redesign individuals' interactions in commerce, public services, politics, and society at large.[23] For instance, it can be applied to prove the existence of a document at a specific time, to know the supply-chain history behind products (clothes, food, diamonds, etc.), to vote electronically, to implement self-executing contracts, to have decentralised domain name systems, decentralized land and commercial registries and more. The great value of this new technology lies in its decentralized architecture, which promotes the redistribution of power from central actors to the peers of a community.[24] Through blockchain, data produced through the web is not processed and stored into a central server,

[19] To know more about the reasons of decentralized failures look at: Narayanan, A., Barocas, S., Toubiana, V., Nissenbaum, H., Boneh, D. (2012) "A Critical Look at Decentralized Personal Data Architectures", Cornell University, New York.

[20] Such as issuance of money and fiduciary functions.

[21] The meaning of "trustless" for blockchain is explained in Chapter II.

[22] "*[Bitcoin is] completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts... With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless*" in Nakamoto, S. (2009) "Bitcoin: A Peer-to-Peer Electronic Cash System". Available at: https://bitcoin.org/bitcoin.pdf.

[23] For a look into the different areas of application of blockchain, see: EPRS – European Parliamentary Research Service (Febr. 2017) "How blockchain technology could change our lives."

[24] Wright, A., De Filippi, P. (2015) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia."

but rather into local devices of users connected to the network. Therefore, in such a decentralized architecture, the users can communicate to one another without intermediaries. Individuals' activities are regulated through the protocols of the network and for their modification the consensus of the majority of the network's nodes is needed. This transparency enables the users to have control over the operations carried out in the platform without having to trust an online operator and its algorithms for the collection, process and storage of data.

1.4 Blockchain and individuals' control over their personal data

In blockchain, like in other decentralized models, the lack of centralized actors (middlemen) calls for a kind of transparency which may collide with its users' privacy. Indeed, the purpose of properly coordinating among the peers of the network requires the availability of data-stores (blocks) to every participant, which includes the metadata relating to the communications occurring in the system.[25] The public character of the blockchain inevitably creates a tension with the privacy of its users since its use requires the storage and exchange of data on a large scale.[26] Indeed, although the use of pseudonyms protects the users' identity, it is still possible to trace back transactions to a specific identity through blockchain analytics techniques.[27] Besides, the blockchain's ledger is characterized by its immutability, meaning that every purchase, transfer or vote become part of a permanent record from which data cannot be erased. The governance of blockchain is highly controversial as it risks to shift the power to new and powerful actors. These and other factors dealt with in *Chapter IV* can turn blockchain technology from a decentralized empowering tool into a new powerful form of surveillance.

1.5 Central questions and sub-questions

Applications of blockchain technology are continuously evolving, as well as technical solutions for the implementation of privacy by-design. The blockchain sector is still in an embryonal stage but, at the same time, it is moving at a very fast pace. The increasing investments of governments and industry giants in this technology are signals of a surge of interest for such a disruptive technology, one that could lead to its future mass adoption.[28] For these reasons, it is paramount to start thinking on the implications for privacy and data protection arising from the adoption of this decentralized

[25] For instance, in Bitcoin, in order to check a bitcoin transaction the node needs access to the previous transactions and, thus, to the financial history of those taking part to the transaction. Only doing so, the node will be able to assess whether the person exchanging the bitcoins actually owns it.

[26] Filipovikj, P., & Holmstedt, C. (2012) "Comparison between centralised and decentralised systems and how they cope with different threats", Abgerunfen am, 22(08), 2013.

[27] Since the Bitcoin blockchain has been often used for illicit purposes, several initiatives have taken place in order to contrast criminal activities. For example, Coinanalytics, Coinometrics, Elliptic, etc.; See also, McKie, S., "The Blockchain Meets Big Data and Realtime Analysis", in Bitcoin Magazine, https://bitcoinmagazine.com/articles/blockchain-meets-big-data-realtime-analysis-1435183048/.

[28] EPRS – European Parliamentary (Feb. 2017) "How blockchain technology could change our lives."

technology in order to preserve the opportunities stemming from it, while reducing its drawbacks for the individuals' fundamental rights and freedoms. Therefore, this research seeks to evaluate whether public blockchain does or does not foster the individuals' control over their personal data as entailed by the right to data protection. This study aims at providing an overview of the blockchain technology and its impact on privacy and protection of data of its users. The purpose is to highlight the blockchain's critical aspects, in particular in light of the GDPR, on which the attention of regulators and software developers should be focused in order to respect the fundamental rights and freedoms of the individuals.

Central and sub-questions:

- How is blockchain providing individuals with more control over personal data? And, at the same time, how may this technology reduce individuals' control?
    - How does blockchain work and which are its main and potential fields of application?
    - What is meant by individuals' control over data under EU data protection law? How can this control enhance the individuals' informational self-determination?
    - Which are the pros and cons of blockchain for users' privacy and data protection? Which challenges does blockchain raise for privacy and data protection under GDPR?

1.6 Methodology

This research is at the same time explanatory and evaluative. It is based on hard and soft law (General Data Protection Regulation; EDPS Opinions; Article 29 Working Party guidelines), as well as on doctrinal legal research and white papers of blockchain developers.

1.7 Overview of chapters

This work is structured as follows. *Chapter I* presents the threats coming from the processing of personal data in centralized architectures and the answers of law regulators and techno regulators to such problems, including blockchain. In order to better understand the blockchain phenomenon and the significant role it can play in the near future, *Chapter II* provides an explanation of the basic functioning of this technology and describes its historical development till its most recent applications. In *Chapter III* retraces the concept of "control" in the European data protection law framework through the analysis of European jurisprudence, academic literature and EU documents. Through the clarification of this concept, in *Chapter IV* is evaluated whether blockchain can or cannot empower its users by providing them with more control over their personal data. Finally, in *Chapter V* the conclusions of this study are drawn.

CHAPTER II

Blockchain Technology. An Overview

At its most fundamental level, Blockchain is a distributed public ledger based on cryptographic technology and (crypto)economic incentives. Its origins trace back to the invention of Bitcoin cryptocurrency, but its evolution goes far beyond digital cash. Blockchain applications, indeed, encompass different spheres from government to culture, from health to supply chains. Therefore, this technology is commonly considered as a potentially truly disruptive tool for a wide range of human activities. Blockchain offers record-keeping functionality as those carried out by banks or government office, but without a trusted third party. This is made possible through the decentralization of the ledger according to which every participant (also called "node") of this technology has a copy of it. Each peer of the blockchain network can ask for transactions to be added to the ledger. Only if accepted by the totality of the participants, these transactions can be added and registered in the ledger. The accepted transactions are bundled in a block, which is finally appended to the last existing one thus creating a chain of blocks or blockchain. Blocks are forged by "miners", a special category of participants and, afterwards, they are validated by all the nodes. Once the block is accepted and added to the chain it becomes public and permanent and it is distributed to all the participants. For this reason, the corruption of the blockchain's ledger would require the corruption of each node's copy of it, therefore making this technology remarkably tamper-proof and trustable.

2.1 Central ledgers

Blockchain is an evolution of ledger systems which are strictly related to hierarchical organizations and commerce. In particular, the history of accounting has ancient origins strictly intertwined with commerce. The most important invention in this field is represented by the *Double-entry bookkeeping system*, the oldest of which is an account of the Republic of Genoa of 1340, the so-called *Messari*. According to this system, every entry to an account must correspond with an opposite entry to a different account, as the name suggests. This system of checks and balances has the merit to decrease errors and to prevent fraud making it hard to be manipulated. Indeed, if the two sides of the accounting equation do not balance, it automatically means that an error or a fraud has occurred. The improvement of systematic bookkeeping has had a significant impact on the growth of modern economy to the point of being considered a relevant factor in the development of capitalism.[29] Banks and governments have always used ledgers to take account of transactions and land ownership to check their legitimacy (i.e. to check that a specific amount of money has not already been spent, or that the house seller is its legitimate owner). Accordingly, users engage in transactions with unknown parties because they all trust a central authority to verify the validity of payments or other transactions.

[29] On this point, Nussbaum, F. (1933) "A History of the Economic Institutions of Modern Europe: An Introduction of "De Moderne Kapitalismus" of Werner Sombart"m New York: Crofts, p. 159; Allen, D. (2011) "The Institutional Revolution: measurement and the economic emergence of the modern world", University of Chicago Press.

The current economical, societal and judicial systems are based on hierarchical organizations. Centralized mechanisms are deemed to create more efficiency because they can better solve information asymmetry and opportunism problems that typically occur in the interaction between unknown agents. Indeed, the assumption behind the economic concept of opportunism is that human beings are moved by self-interest that spurs them to take advantages whenever possible. This risk is higher when transactions occur between unknown parties.[30] Therefore, basically what centralized systems do is to generate trust in the interactions among strangers.[31] Reliability on centralized authorities is supported by the maintenance of accurate accounting systems: the ledgers. Through this technology, it is possible to keep records of relevant information such as property, identity, licenses, etc., necessary to overcome the aforementioned economic opportunism. However, centralized solutions also present several drawbacks. They can be costly (i.e. bank and notary fees, taxes to access public ledger, etc.), slow (i.e. money transfer), vulnerable to tampering (i.e. a central server is easier to attack than a distributed one), black-boxed (access is controlled by the central authority). Instead, blockchain not only allows the overcoming of opportunism in the absence of a centralized institution through its record-keeping functionality, but it also claimes to be able to overcome the above mentioned typical flaws of centralized accounting systems.

2.2. The first wave of blockchain. Cryptocurrencies

The first application of blockchain dates back to the invention of Bitcoin, the first and most spread decentralized cryptocurrency and online payment system. This invention has finally solved the long-standing problem of *double-spending* in peer-to-peer electronic cash systems, a matter that has typically required the intermediation of third actors in the e-commerce. Indeed, due to the easy possibility of copying digital assets such as digital cash, trusted third parties (banks or other financial intermediaries) were necessary in order to confirm that a certain amount of digital cash had not already been spent.

In 2008, Satoshi Nakamoto, the inventor of Bitcoin, published a paper theorizing a way to avoid double-spending in peer-to-peer transactions without central authorities. This solution entailed the creation of a new digital currency governed by the Bitcoin protocol and a public ledger to record the chain of transactions. The implementation of this new system did not require any new technology, being a combination of already existing ones, namely BitTorrent peer-to-peer file-sharing and public-key cryptography.[32] Blockchain is the public cryptographically secured and distributed ledger that underpins Bitcoin transactions. This ledger, as the name suggests, consists of a chain of blocks built on a peer-to-peer network, which encompasses all those created from the beginning of the network.

[30] The literature on economic opportunism is vast. Specifically, one influential economic theory on opportunism is the Transaction Cost Economics. A suggested reading on this topic is: Moschandreas, M. (1997) "The Role of Opportunism in Transaction Cost Economics", in Journal of Economic Issues, Vol. 31, No. 1, pp. 39-57.

[31] Williamson, O. E. (1973) "Markets and hierarchies: some elementary considerations", American Economic Review 63(2): 316-25; Williamson, O. E. (1985) "The Economic Institutions of Capitalism", New York: Free Press. The hesitation in the engagement in transactions has been studied by the transaction cost theory (TCT) field, also known as the institutional economics.

[32] Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System". Available at: https://bitcoin.org/bitcoin.pdf.

Each block contains the answer to a complex mathematical puzzle, a reference to the precedent block (its *hash*) and a list of verified transactions from the previous one. A new block of data is appended to the end of the chain in a chronological order once the network has achieved consensus on the validity of the transactions listed in the new one. Once the block is added, it cannot be removed. The blockchain is recorded in a distributed manner by a decentralized network of users' computers (*nodes*), which periodically synchronize. Accordingly, this technology solves the double-spending problem through the recording of coin ownership in a public ledger which requires prior distributed consensus from certain computers of the network or certain nodes (*miners*) through the *Proof-of-Work*, which is the mechanism standing at the core of this technology.[33] According to this mechanism, a subset of nodes called miners must solve complex mathematical puzzles that turn the information contained in the block into a unique sequence of numbers and letters (*hash*) that acts as a unique fingerprint. As soon as the majority of the network's nodes approves the mathematical solution, the transactions are recorded in the ledger. Accordingly, the need for a central authority disappears thanks to the activity carried out by miners who, through cryptographic techniques, confirm the legitimacy of the transactions after making sure that double-spending does not occur.[34] At this point, another well-known problem in computer science arises, the so-called *Byzantine General Problem*[35], characterized by the following problems:

(a) how to reach consensus in distributed computer systems among unrelated parties; and

(b) how to be able, at the same time, to resist attacks from malicious actors.

Blockchain technology addresses the first issue through economic incentives. Miners get involved in mining operations, although this requires a high consumption of computational power, because of the rewards gained from each transaction approved, which corresponds to a certain amount of Bitcoin.[36] This incentive encourages miners to reach a consensus and to forge new blocks. The second concern is solved with a probabilistic approach that combines the inclusion in every hash of the previous hash, together with the employment of a peer-to-peer distributed timestamp server that works as a computational proof of the chronological history of transactions. As a result, every tampering attempt to even one single block can be easily detected. Indeed, the corruption of one block would create incoherence among the tampered block and those that precede it and follow it. In order to succeed, malicious actors would need to change all the blocks of the chain. In order to let the tampering being

[33] Apart from Bitcoin, there are other mechanism to achieve consensus, such as the Proof-of-Stake.

[34] *Miners* are a subset of nodes. *Nodes* have the tasks to verify the validity of the transactions in the blocks received, to store them and afterwards to broadcast them to other nodes who will relay the transactions to other nodes, and so on. Some of these nodes are also miners who perform additional work. In particular, miners are those who choose which valid transactions can be added in the block. the transactions to be included in a block. Look at: https://bitcointalk.org/index.php?topic=1734235.0.

[35] In this problem, it is assumed that three divisions of the Byzantin army are camped in the surroundings of a city that they plan to attack. The generals can communicate only through a messenger, but one of them may be a traitor. The problem is how to reach a consensus on the same plan of attack avoiding that the traitors will cause the adoption of the wrong plan. This issue is explained in: Lampert, L., et al., (1982) "The Byzantine General Problem", 4 ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS, p. 382.

[36] Each block includes thousands of transactions.

unobserved, this should be done very fast. Indeed, as pointed out by Nakamoto, "the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added."[37] In other words, the more blocks in the chain the more effort to tamper all of them without being noticed. Moreover, the computers of the networks (nodes) periodically synchronize with each other to confirm that they share the same database, making control over the correctness of the ledger spread all over the network.[38] Therefore, the more nodes in the networks, the more "trustless" the system become, which means that users do not need to trust each other or an intermediary to engage in transactions but can rely on the blockchain's protocol software system (consensus mechanism built upon crypto-economic incentives, cryptographic techniques and a public distributed ledger so that each participant can have a copy of it). Therefore, in blockchain, crypto proof replaces traditional trust.[39]

The creation of a large scale of decentralized trustless transactions is the remarkable key innovation of blockchain.[40] Through the mechanism described, Bitcoin can be used to buy and sell over the Internet without intermediation. The only three elements needed are:

- a wallet software to run on the computer that allows the management of Bitcoin;
- an address to send and receive coins; and
- a private key to securely send coins.

So far, also many other cryptocurrencies have been developed such as Peercoin, Factom, Zcash, Ether, Namecoin, Equinox, etc.

2.3 The second wave of blockchain. Smart contracts

As pointed out by Satoshi Nakamoto in 2010, "*the design supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third-party arbitration, multiparty signature, etc*."[41] Indeed, the decentralization of money and payment is

[37] Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System". Available at: https://bitcoin.org/bitcoin.pdf. On this point, see also: http://www.coindesk.com/information/how-bitcoin-mining-works/

[38] Nakamoto, S., *Ibidem*, p. 4; more technical details can also be found in other white papers. In particular, see: Buterin, V. (2014) "Ethereum: A next-generation smart contract and decentralized application platform" Available at: https://github.com/ethereum/wiki/wiki/White-Paper.

[39] Nakamoto, S. (2009) "Bitcoin Open Source Implementation of P2P Currency", P2P FOUNDATION. Available at: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source ; However, in case the attacker gain control of even 40% of the network's computing power, this would have good probabilities to succeed, see: Hajdarbegovic, N. (Jan 9, 2014) "Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack." Available at: https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/.

[40] Swan, M. (2015) "Blockchain: Blueprint for a New Economy", O'Reilly Media, p. X; The Economist, "The promise of the blockchain. The trust machine", 31 october 2015. Available at: http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

[41] Nakamoto, S. (2010) "Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG." Bitcointalk. Available at: https:// bitcointalk.org/ index.php.

definitely only one of the possible forms of decentralization allowed by blockchain. Many other non-currency-related applications can be developed upon blockchain. A public distributed transaction ledger can be functional for the registration, confirmation and transfer of a wide range of different kinds of contracts and properties in various areas, such as:

- financial transactions (bonds, crowdfunding, mutual funds, etc.);
- public records (land and property titles, marriage and death certificates, vehicle registrations, business licenses, etc.);
- identification (identity cards, voter registration, driver's licenses, etc.);
- intangible assets (patents, trademarks, copyrights, domain names, etc.);
- and many more.[42]

Thus, although cryptocurrencies are the most popular and mature application of blockchain, they are not the unique ones. Since blockchains are databases that can record everything that can be coded into it, this technology can find application with hard assets (car, home, computer) as well as soft ones (intellectual creations) and, in general, with whatever that can be translated into mathematical language making possible the management of assets through blockchain after their registration. The owner of the private key would manage the ownership of the blockchain-encoded properties, namely *smart properties*, whose relating transactions can be regulated through *smart contracts*. The latter involves transactions - more sophisticated than buying and selling - agreed between one or more parties, defined and executed by the code. This transaction is stored in the blockchain, thus, making this kind of contract a trustless one. There is no need for trust between parties due to the self-enforceability of smart contracts. Indeed, in smart contracts a set of information is coded and when specific conditions embedded into it are met, they will automatically be followed by the execution of those actions that have been agreed on by the parties and encoded in the blockchain. For instance, one application could entail the registration of death as an automatic trigger of the distribution of inheritance to a specific person.

Smart contracts can be used to facilitate the execution and the enforcement of contract conditions without having to refer to a central authority since its execution is based on a specific programming language in which the contract has been translated (obligations, penalties). Once the draft of the smart contract is ready, it can be directly uploaded as a block in the blockchain to be executed. Since the code both defines and enforces the contract, decentralized applications can even interact without the need for human intervention. This interaction is possible through Decentralized Autonomous Organizations (DAOs) that involve the translation in mathematical language of a series of rules for an organization bounded to these instructions. These organizations are run by a set of governance rules (decision-making process) automatically enforced in the blockchain. Moreover, further advancements in blockchain technology also make the interaction between multiple interconnected smart contracts possible in DAOs.

[42] This list is taken from Swan, M. (2015) "Blockchain: Blueprint for a New Economy", O'Reilly Media, position 474 (ebook).

The concept of smart contract has been outlined for the first time in 1994 by the American cryptographer Nick Szabo.[43] However, the IT infrastructure of that time could not support such a technology. Years later, blockchain has enabled the application of smart contracts through its further development: the realization of a general infrastructure on which every kind of blockchain and protocols can be written and run. Ethereum is the most advanced project of this kind. This is a general-purpose cryptocurrency platform upon which it is possible to develop programs for any (reasonable) computational problem.[44] Through Ethereum autonomous applications can be built and operated autonomously on the blockchain.[45] As Grace Caffyn puts it, "*Arguably the most ambitious 'crypto 2.0' project to date, and the third-largest crowdfunded project of all time, Ethereum is aiming to create a new universe of programmable contracts, powered and secured by its own proof-of-work blockchain. Grand in scale and exible by design, it aims to decentralize pretty much anything on the Internet. «What bitcoin does for payments, Ethereum does for anything that can be programmed…".*[46] As well, Ethereum's co-founder emphasises the potential of this technology even more, defining it as a magic computer: "*A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publically visible, and which carries a very strong crypto-economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies. ... Blockchains are not about bringing to the world any one particular ruleset, they're about creating the freedom to create a new mechanism with a new ruleset extremely quickly and pushing it out. They're Lego Mindstorms for building economic and social institutions*."

2.4 Permissioned and permissionless blockchain

An important categorization of blockchain types takes into account whether authorization is needed to access the blockchain as well as for the nodes of the network to act as verifiers. According to this distinction, blockchain systems are divided in three main categories:

- permissionless and public blockchain;
- permissioned and private blockchain;
- consortium blockchain.

[43] Szabo, N. (1994) "Smart Contracts"; also, for a further development of this idea, see: Szabo, N. (1997) "The Idea of Smart Contracts."

[44] More technically, this means that Ethereum delivers Turing-complete scripting language and platform. See: Swan, M., (2015) "Blockchain: Blueprint for a New Economy", O'Reilly Media, position 808 (ebook); https://ethereum.stackexchange.com/questions/2464/what-does-it-mean-that-ethereum-is-turing-complete.

[45] Buterin, V., et al. (2016) "A Next Generation Smart Contract and Decentralized Application Platform", Ethereum White Paper, Available at: https://github.com/ethereum/wiki/wiki/White-Paper.

[46] CoinDesk, "Ethereum Launches Long-Awaited Decentralized App Network", 30 July 2015, http://www.coindesk.com/ethereum-decentralized-app-network-launch/

Permissionless and public blockchain. The access to the blockchain is open to anyone in terms of carrying out transactions and participating in the consensus process. This kind of blockchain is also considered the most decentralized one.

Permissioned and private blockchain. In this kind of blockchain the participation is restricted assuming the shapes of a traditional centralized system combined with cryptographic means. Indeed, the entity running such blockchain decides the rules, validators are pre-selected and, therefore, are known.[47]

Consortium blockchain. The consensus mechanism is attributed to a specific and pre-selected set of nodes, though the possibility to read the blockchain may be open to everybody or only to participants. This kind of blockchain is generally understood as partially decentralized.

2.5 Further applications

Smart contracts allow the decentralization of trustless transactions, worldwide and on a large scale. These can encompass different kinds of interaction, not only human-to-human but also human-to-machine and machine-to-machine as it is described below.

Blockchain for the Internet of Things. Blockchain, which is a ledger of potentially everything, can be applied to the Internet of Things (IoT), an internet of potentially everything since almost every kind of device and tools can be connected to the Internet. In the current IoT ecosystem, devices are connected through the employment of cloud servers with huge storage capacities. However, in the future this computing capacity will not be enough when the amount of connected devices will be massive. Blockchain recording metadata could become the solution. Besides, the collection of all the data produced by the IoT by central companies constitutes a high risk for the users' privacy, which could also be solved using decentralized technologies such as blockchain. Blockchain for the IoT will permit machines, registered in the ledger, to exchange information and execute smart contracts. It will reduce the cost associated with the maintenance of large data centers, it will prevent central collection of personal data and single node failure, therefore providing more security.[48] The combination of blockchain and IoT is seen as very powerful, one that can pave the way for new business models and applications.[49] Initiatives going in this direction are carried out for instance by IBM and Samsung, Filament, Chain of Things, and many others, though still in an early stage.[50] At

[47] Buterin, V. (August 7th, 2015) "On Public and Private Bockchain". Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[48] Compton, J. (Jun 27, 2017) "How Blockchain Could Revolutionize The Internet of Things". Available at: https://www.forbes.com/sites/delltechnologies/2017/06/27/how-blockchain-could-revolutionize-the-internet-of-things/#6697ab2e6eab

[49] Bozic, N., Pujolle, G., Secci, St. (2016) "A tutorial on blockchain and applications to secure network control-planes", Smart Cloud Networks & Systems, pp. 1- 8.

[50] To know more about the application of blockchain in the Internet of Things, look at: Conoscenti, M., et al (2016) "Blockchain for the Internet of Things: A Systematic Literature Review", The 3rd International Symposium on Internet

the same time a ledger recording every aspect of our daily life from fridge usage to health devices will also make the blockchain a tool for the control of everything.

Blockchain for AI. Another application of blockchain consists of using it to formulate thinking through algorithms.[51] Faster analysis of huge amounts of data of the artificial intelligence together with blockchain technology can be the beginning of a new paradigm. For instance, IBM is investing to converge blockchain, artificial intelligence and IoT to create a "Watson-powered blockchain." This platform filters device events and transmits to the blockchain (smart contracts) only the relevant data translated in the format needed by the blockchain contract APIs.[52] Accordingly, devices will be able to communicate with each other, requiring the supply of a specific product or a technical problem to be solved, and so on.

Blockchain for public services. Blockchain technology can stir the rethinking of public services, as noted by the UK Government that published a report presenting potential applications of blockchain to support compliance, to reduce fraud, to better manage citizens' identity, property and land registries and even more.[53] Its Department for Work and Pensions is experimenting welfare payments through blockchain.[54] The Estonian government is launching a blockchain-based system for 1 million patient healthcare records.[55] Ghana and other African countries are using blockchain to keep record of land registries.[56]

---

of Things: Systems, Management and Security, Agadir (MAR); Christidi, K. (2016) "Blockchains and Smart Contracts for the Internet of Things", Access IEE, vol. 4, pp. 2292 – 2303.

[51] Swan, M. (2015) "Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization)", http://www.the-blockchain.com/docs/Blockchain%20Thinking%20-%20The%20Brain%20as%20a%20DAC%20-%20Decentralized%20Autonomous%20Organization.pdf.

[52] IBM – International Business Machines - "Watson Internet of Things". Available at: https://www.ibm.com/internet-of-things/platform/private-blockchain/; del Castillo, M. "IBM Watson is Working to Bring AI to the Blockchain", CoinDesk, 5 April 2016. Available at: http://www.coindesk.com/ibm-watson-artificial-intelligence-blockchain/ ; CFP: Blockchain Applications in Artificial Intelligence And Cognitive Science, 6 April 2016. Available at: http://www.coindesk.com/ibm-watson-artificial-intelligence-blockchain/

[53] The UK Government Chief Scientific Adviser (2016) "Distributed Ledger Technology: beyond blockchain."Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[54] AM Eastern Daylight Time, "GovCoin Systems Implements Social Welfare Payments Distribution Trial for UK's Department for Work and Pensions", 7 July 2016. Available at: http://www.businesswire.com/news/home/20160707005803/en/GovCoin-Systems-Implements-Social-Welfare-Payments-Distribution

[55] Palmer, D. (2016) "Blockchain Startup to Secure 1 Million e-Health Records in Estonia". Available at: http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/

[56] BlockchainNews, "Blockchain Startup Bitland to Implement Blockchain Property Records in Ghana", 19 May 2016. Available at: http://www.the-blockchain.com/2016/05/19/blockchain-startup-bitland-to-implement-blockchain-property-records-in-ghana/ ; BitLand. Available at: http://landing.bitland.world .

Other applications. Many businesses are using blockchain technology. To name some of these: *BitStamp*, the first European bitcoin exchange platform with a banking license;[57] *Ubiquity*, the first blockhain-secured platform for real estate recordkeeping;[58] *Ascribe*, a record of ownership on creative works;[59] and more.

[57] Bitstamp. Available at: https://www.bitstamp.net.

[58] Ubiquity. Available at: https://www.ubitquity.io/site/index.html.

[59] Ascribe. Available at: https://www.ascribe.io.

Chapter III

The right of individuals to have control over their personal data

3.1 The right to informational self-determination and the individuals' control over personal data

"*Natural persons should have control of their own personal data*" Recital (7) of the Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR) affirms. More control to individuals is often seen as the solution to threats coming from the processing of personal data on a massive scale.[60] Indeed, according to one of the several definitions relating to privacy, this should be considered in terms of "control"[61] with regard to informational privacy.[62] According to this view, privacy is preserved when the individual is put in the condition to self-manage the information concerning him or her. Control over personal data is therefore conceived as an expression of the individuals' self-determination. The assumption underlying this view is that individuals are deemed able to consciously decide for themselves on how to use their data, meaning that this decision should be left to them. Accordingly, individuals are considered able to determine what is good for themselves when sharing their data and should be empowered in order to effectively exercise their control over which data to disclose, to whom, how and when.[63] It is about deciding for oneself about to what extent and to whom to communicate thoughts, emotions, habits, and so on. According to one definition, privacy as control is *"[…] the view that a right to privacy is the control an autonomous human being should have over his or her personal information, regarding its collection, processing and further uses, including onward transfer*."[64] Other conceptions of privacy exist[65] mainly sharing a common theoretical assumption: the individual's autonomy and the self-direction of one's life.[66] Accordingly,

[60] Peppet, S. R. (2011) "*Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*", in *Northwestern U. Law Rev.*, Vol. 105, p. 1183.

[61] Tavani, H. T. (2007) "Philosophical theories of privacy: Implications for an adequate online privacy policy", Metaphilosophy 38(1):1-22.

[62] On informational privacy and the difference between privacy and data protection is clear in: Hustinx, P. (2005) "Data Protection int he European Union", Privacy & Informatie, pp. 62-65.

[63] Fuchs, O., (2011), "Towards an alternative concept of privacy", JICES, Vol. 9, No. 4, p. 223; Solove D. J. (2013), "Privacy Self-Management and the Consent Paradox", in: Harvard L. Rev., Vol. 126, pp. 1880-1903.

[64] Birnhack, M. D. (2011) "A Quest for A Theory of Privacy: Context and Control", Jurimetrics, Vol. 51, No. 4.

[65] About this point see: Solove, D. J. (2009) "Book Notes: Understanding Privacy", Osgoode Hall Law Journal 47.4. In this book the author proposes the classification of privacy definition as it follows: (1) the right to be left alone; (2) limited access to the self; (3) secrecy; (4) personhood; and (5) intimacy.

[66] Lazaro, C., Le Metayer, D. (2015) "The control over personal data: True remedy or fairy tale?", ScriptEd, Vol. 12, Issue 1.

privacy is generally conceived as individualistic since it puts the individual at the centre, and active because it aims at the construction of the self. [67]

The conception of privacy as control is related to the right to informational self-determination upon which data protection regime is developed. One of the first and most known description of the right to informational self-determination traces back to the famous "Population Census Decision" ("Volkszählungsurteil") of the German Federal Constitutional Court (Bundesverfassungsgericht or BVerfG) in 1983.[68] In this ruling, based on Article 1 on human dignity and Article 2 on personality right of the German Basic Law,[69] the Court articulated the right to informational self-determination as "*the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others.*" According to the BVerfG, the automated processing of personal data deriving from the modern sophisticated processing of data represented a danger for the values of Basic Law lying on "*the value and the dignity of the individual being a self-determined member of a free society*."[70] The right to informational self-determination therefore encompasses both individuals' autonomy - privacy is "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others*"[71] - and dignity. The value of human dignity stressed in the Court's decision means to highlight the protection of the individuals' interest in being a person and developing his or her own personality.[72] One's control over personal data involves knowledge about which data about oneself is shared, for what purposes, to what extent as well as the management of one's personal data. Through control, the individual should concretely be the author of the view that society has on him or her in the digital space. It follows that control is a means for the realization of the individual's autonomy and respect of his or her dignity. The individual's control over personal data existing about him or her, thus, constitutes a precondition for living a self-determined life, an essential element of the "informational self-determination."[73] Among data protection scholars, the concept of informational self-determination and that of data protection are closely linked.[74]

---

[67] Rouvroy, A., Poullet, Y (2009), "The Right to Informational Self-Determination and the Values of Self-Development: Reassessing the Importance of Privacy for Democracy", in: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds.) "Reinventing Data Protection?", Springer, Dordrecht, p. 8.

[68] *BVerfGE 65,1 – Volkszählung*.

[69] Basic Law for the Federal Republic of Germany, https://www.btg-bestellservice.de/pdf/80201000.pdf.

[70] Dix, A. (2011) In "Bundesdatenschutzgesetz", Simitis, S. (ed.) 1207–1487, Baden-Baden: Germany: Nomos.

[71] Westin, A. (1967) "Privacy and Freedom", Bodley Head, London, p. 7.

[72] In particular, "the right to privacy protects the individual's interest in becoming, being and remaining a person.", in Reiman, J. H. (1989) "Privacy, Intimacy, and personhood", in Philosophical dimensions of Privacy, Schoeman, F.D. (ed.), p. 314. See also, Rubenfeld, J. (1989) "The Right of Privacy", 102 *Harv. Law Rev.*, pp. 737–807.

[73] Rouvroy, A., Poullet, Y (2009), "The Right to Informational Self-Determination and the Values of Self-Development: Reassessing the Importance of Privacy for Democracy", in: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds.) "Reinventing Data Protection?", Springer, Dordrecht, p. 51.

[74] This principle of "informational self-determination" is conceived to be the justification ground for the european data

3.2 Individuals' control over personal data in EU documents

The concept of individuals' control as functional for the protection of privacy is not only mentioned in Recitals of the GDPR, but also in other EU documents. In "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century", a communication by the European Commission of 2012, some explications are provided about the content of the individuals' empowerment through their control over their personal data are provided. In this document, the control to which the GDPR – at that time just a proposal – is aiming means "*to strengthen rights, to give people efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively*." In particular, to improve individuals' ability to control their data the Commission proposes tools for the individual such as explicit and freely given consent, the right to information, the right to easily access one's own data, the right to be forgotten, the right to data portability and the right to object to automated processing. At the same time for the full exercise of individuals' rights, the Commission proposes complementary interventions such as strengthening independence and powers of national data protection authorities, enhancing administrative and judicial remedies in case of violation of rights. As well, another fundamental aspect taken into account by the Commission includes the reinforcement of data security also through the encouragement of privacy-by-design and by-default and the introduction of data breach notification. Finally, the designation of a Data Protection Officer and the need to carry out a Data Protection Impact Assessment are introduced in order to increase the accountability of data controllers and processors.[75] From this overview it emerges as the core of individuals' empowerment those rights and conditions that allow the individual to express actively his or her choices about the processing of his or her personal data:

- right to information;
- explicit and freely given consent;
- right to access, correction, and erasure;
- right to object to automated processing and to obtain human intervention;
- right to be forgotten;
- right to data portability.

Another EU document specifically referring to the importance of having control over personal data is the brochure named "Take control of your personal data."[76] Here, several images express messages

protection regime. On the meaning of informational self-determination as the individuals' control over personal data as a pre-condition to a self-determined existence, look at: Buitelaar, J. C. (2012) "Privacy: Back to the Roots", German Law Journal, 13/3, 171-202; and, Rouvroy, A., Poullet, Y (2009), "The Right to Informational Self-Determination and the Values of Self-Development: Reassessing the Importance of Privacy for Democracy", in: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds.) "Reinventing Data Protection?", Springer, Dordrecht, pp. 45-76.

[75] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committe and the Committes of the Regions, "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21th Century, COM(2012) 9 final, Brussels, 25.01.2012, p. 6.

[76] European Commission, "Take control of personal data", Available at: http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf.

relating to the empowerment of the individual through control over data allowed by the upcoming GDPR. Control is expressed in terms of knowing who to trust when sharing personal information and who to contact in order to exercise the rights of data protection, to have the possibility to read in a clear language the relevant information about privacy, to have data protected by all sides unless the individual opts for changing the settings, and to have the opportunity to remove data and to transfer them to another service provider.

European Commission, "Take control of personal data", Available at: http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf.

Another body of literature of the European Union about control over data comes from the European independent data protection authority, the European Data Protection Supervisor (EDPS). This authority is often referring to the need of granting more individuals' control over their data. In particular, among the essential elements for a sustainable development of big data the authority includes the need for a high degree of control over how data are used. The EDPS associates control over data to the rights of access and to data portability, as well as to effectiveness of opt-out mechanisms, privacy-by-design and more.[77] The European supervisor encourages the development of technologies that empower the individuals and enable him or her to control the personal data shared

[77] EDPS - European Data Protection Supervisor (2015), Opinion 7/2015, "Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability, p. 4. Available at: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.

aiming at providing individuals with tools that allow avoiding invasive tracking and consequent data analytics.[78]

3.3 The GDPR and the individuals' empowerment through control

In line with the landscape described above, within the GDPR the concept of control refers to a first kind of elements expressed in terms of equipping individuals with "micro-rights" relating to different stages of data processing (right to access, right to data portability, right to be forgotten, etc.). Nonetheless, this empowerment is also linked to another kind of elements that encompasses technical and organizational measures such as the enforcement of security measures, higher responsibility and accountability of data controllers and processor (i.e. appointing a data protection officer), the introduction of the privacy-by-design and by-default principles, the obligatory of the data protection impact assessments in some cases, the enhancement of administrative and judicial remedies (i.e. the coherence mechanism, independency of data protection authorities) and the data breach notification. All these measures aim at creating a privacy-friendly environment through technical and organizational elements. What emerges is that the GPDR pursues the individuals' empowerment providing them not only with direct tools for data subjects, but also creating a privacy-friendly environment through technical requirements to shape the data processing architecture in the respect of the fundamental rights and interests of the individuals. Therefore, the GDPR aims at providing individuals with more control through the imposition of a higher level of transparency and the strengthening of rights and introduction of new powerful ones.[79] Among the principles, rights and requirements enshrined in the GDPR there are some that have been introduced or officially recognized for the first time in order to empower the individuals. The attention will be focused on some of the most relevant novelties that, on one side, fall under the umbrella of "privacy by control" by the individuals (the right to data portability and the right to be forgotten) and, on the other side, on those principles inspiring "privacy by architecture" (the principles of privacy by-design and by-default).

Right to data portability. The right to data portability (RDP) is enshrined in Art. 20 of the GDPR and encompasses both the right to obtain a copy of personal data in a "structured, commonly used, machine-readable and interoperable format" and the right to transmit these data to another controller "without hindrance" (Art. 20(2) GDPR). Nevertheless, where "technically feasible", the transfer should be carried out directly by the data controller. In line with the GDPR's purposes, the RDP empowers individuals' control over their data. In this sense, the freedom to choose the data controller service provider that will store and process personal data is in line with the right to informational self-determination. According to this view, the right to data portability enables the user to actually manage her or his personal data enabling an effective self-governance and self-direction of one's life. As also

[78]EDPS - European Data Protection Supervisor (2016), Opinion 9/2016, "EDPS Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data". Available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

[79] EDPS - European Data Protection Supervisor (2016), Opinion 9/2016, "EDPS Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data". Available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

highlighted by the Article 29 Data Protection Working Party, this right enhances the individuals' control over the personal data that concern them.[80] Indeed, the individual's choice to stop using a platform (unless in case of multi-homing) and to switch it in favour of another one is supported by the interoperability of the data format and the requirement to have the transfer carried out "without hindrance." Moreover, the data subject has the extra possibility to have the fulfilment of this shift carried out from one platform to another one. In this way, data subjects can use their personal data for their own purposes across interoperable applications (obtaining new or additional services, selling them spontaneously, etc.). The freedom to choose what data controller service provider should store and process personal data is therefore an expression of the right to self-determination. Data portability has the merit to reinstate a more balanced relationship between businesses and individuals providing to the latter more control over his or her personal data.[81]

Right to be forgotten. At its foundations, the right to be forgotten is the right for natural persons to have personal data deleted after some time. In Europe, this right has been firstly recognized in France as the *droit à l'oubli*. More broadly, it traces back to the right to respect for private life (Art. 8 of the European Convention on Human Rights) and the right to data protection (Art. 8 of the European Charter of Fundamental Rights and Freedoms). Although this right has been formally introduced by the General Data Protection Regulation (Art. 17), already the European Directive on Data Protection (Dir.95/46-EC) set forth the principle according to which personal data should be kept only for as long as they are necessary for the purpose of the collection (Art. 6e), as well as that the person can ask for the deletion of personal data that are no longer necessary (Art. 12). Moreover, stretching the 1995 Directive's provisions, the Court of Justice of the European Union (CJEU), in 2014, already recognized the existence of the right to be forgotten establishing its general principle in the notorious *Google Spain* case. The CJEU recognized the obligation of search engine operators in removing links to webpages showed among the results of a query when they are "inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes of the processing at issue."[82] However the publications in question were not illegitimate by themselves and are still published. The Court also specified that the right to have personal data deleted is not an absolute one. The complainant needs to demonstrate the lack of a "preponderant interest of the general public" in having access to the information.[83] The underlying rational of this right is to allow individuals to full self-determine their lives, without having to be periodically associated with past actions relating to a long time ago.[84] It is also described as the "right to remorse" or "to change one's mind" and "not to be permanently

[80] Article 29 Data Protection Working Party (2016), "Guidelines on the right to data portability", p. 4.

[81] *Ibidem*.

[82] Google Spain, Case C-131/12, p. 94. Available at: http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

[83] *Ibidem* p. 100(4).

[84] Lynskey, O. (2015) "Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez", Modern Law Review, 78(3), pp. 523-534. Available at: http://eprints.lse.ac.uk/61944/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Lynskey%2C%20O_Control%20personal%20data_Lynskey_Control%20personal%20data_2015.pdf.

remembered one's past."[85] The right to be forgotten is the expression of the fundamental right to have control over certain aspects of one's life, such as making choices and taking informed decisions.[86] Indeed the information to which others have access defines our social identity. The control over personal data allows to show different aspects of the self to the chosen people depending on the social context. This right to informational self-determination has been recognized and protected as a right to the protection of personal data.[87] However, this right is not an absolute one and needs to be balanced with other public or private interests. The fast development of information and communication technology (ICT) has played a determining role in the need to rethink how to balance free dissemination of information with the individual self-determination. Indeed, for the first time in history spontaneous public communication remains long after having been expressed, therefore, having a wider impact due to the access to an undefined, and potentially high, number of people.

Privacy-by design. This principle refers to taking privacy into account from the beginning of the engineering process towards all the following steps. It is explicitly enshrined in Art. 25 of the GDPR, but its concept has its origins in 1990s in a report on privacy-enhancing technologies presenting guiding principles on the topic by the Information and Privacy Commissioner of Ontario, the Dutch Data Protection Authority and the Netherlands Organization for Applied Scientific Research.[88] The GDPR does not provide a punctual definition of this principle because of the technology neutral principle according to which this Regulation should apply to all kinds of technology and not only to a specific one.[89] Due to a gap in the legislation, the obligation to process data in respect of privacy by design is only set up on the data controller who have to detect which measures are adequate in order to implement privacy from the very first steps of the design of a technology, and not also on the developers and providers of software and infrastructures, who are only encouraged to do so. Explicitly mentioned as potentially appropriate measures are data minimization and pseudonimisation. Recital (78) of the GDPR states that "*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.*" Privacy by design is

[85] De Terwangne, C. (2013) "The Right to be Forgotten and the Informational Autonomy in the Digital Environment", European Commission Joint Research Centre, p. 6.

[86] The right to self-determination has been explicitly recognized as part of the right to respect of private life in ECtHR, *Evans v. United-Kingdom*, 7 March 2006, req. N. 6339/05 with the wording of "a right to personal autonomy."

[87] Charter of Fundamental Rights of the European Union, 2000/C 364/01, Art. 8. Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[88] Information and Privacy Commissioner, Ontario (Canada) and Registratiekamer (Netherlands), Privacy-Enhancing Technologies: The Path to Anonymity (Volume I), 1st August 1995. Available at: http://tinyurl.com/yenjgns.

[89] Maxwell, W. J., Bourreau, M. (2015) "Technology Neutrality in Internet, Telecoms and Data Protection Regulation", in Computer and Telecommunications Law Review.

also closely linked to the principle of data minimization.[90] According to GDPR "*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing*" (Art. 25).

Privacy-by-default. Default settings must protect the privacy of individuals according to this principle. Exemplary is the opt-in approach. In more details, the data controller has to carry out measure for "*ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*" (Art. 29 GDPR).

[90] Hustinx, P. (2010) "Privacy by design: delivering promises", in Identity in the Information Society, Volume 3, Issue 2, pp. 253-255.

CHAPTER IV

Privacy and data protection implications of blockchain technology

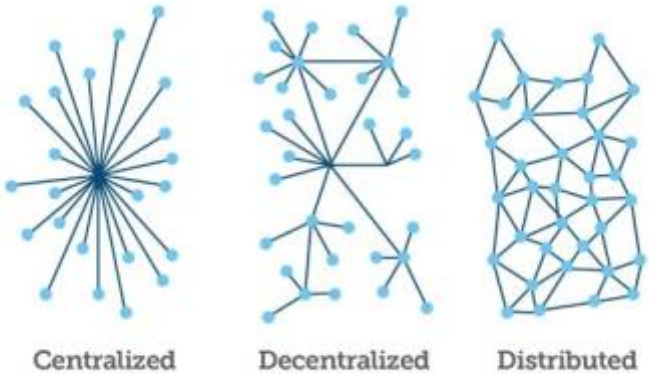
As already seen in this work, decentralization attempts have meant so far to contrast the growing centralization of the Internet where communication constantly leaves traces. What is highlighted in this Chapter is that, on one hand, blockchain can provide more privacy and autonomy to individuals than centralized systems but, on the other hand, it raises new challenges that risk to convert this technology into an intrusive one. The main implications for the privacy and data protection deriving from permissionless public blockchain are therefore presented.

4.1 Blockchain and the benefits for the individuals' control

Blockchain can have a positive impact in terms of increasing individuals' control over their personal data, at the core of the right to data protection, thanks to: the lack of a central party, the high level of transparency and the deployment of encryption and pseudonymization techniques.

Lack of a central party. Centralized platforms, by design, collect information about the users' online activity. Indeed, as seen in *Chapter I*, personal data represent a core aspect of the digital economy and its concentration in the hands of one player increases the power of those who, legitimately or not, exercises control over it profiting of data lock-in, in-depth knowledge of customers' purchasing trends, behavioural advertisements, etc.[91] Every time an activity requiring central intermediaries is carried out, the position of power and related profits is reaffirmed. One of the main benefits of the lack of a central point of control over the network's flow of information is that surveillance is more difficult to be achieved. In the blockchain, indeed, there is not a central party with extended control over individuals' data deriving from storing and processing activities. This design should be beneficial for its users' control over their data because they don't have to fear the concentration of their data and possible profiling by a third party providing the service. With a highly decentralized architecture such as blockchain, the digital *panopticon* should not take place because of the lack of a central point of control in its architecture.

[91] For example, Facebook carried out psichological experiments to study how the users' news feed manipulation can influence users' feelings. All this without the subjects of the study being aware of it. See: Goel, V., "Facebok tinkers with users' emotions in news feed experiment, stirring outcry", The New York Times, 29 June 2014. Available at: https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html?_r=0 .



https://www.linkedin.com/pulse/blockchain-distributed-ledger-technology-david-cox

Another privacy concern of centralized client-server model overcomed by blockchain is the susceptibility to attacks by third parties.[92] In contrast, blockchain is a resilient technology that provides high security especially in the prevention of data tampering and computer's failure thanks to the distributed nature of the ledger. As well, blockchain's irreversibility makes this system incorruptible since any change of one block affects all the others in the chain. Consequently, an incompatibility between a corrupted block and the others will already reveal a malicious attempt. Therefore, blockchain prevents eventual leak of personal data or loss of availability of them which could weaken the control individuals should have over their data.

Transparency. In blockchain, participants know what data is collected about them and how they are processed. This is due not only to the transparency of the ledger in which data relating to the transactions are recorded, but also to the transparency of the blockchain's protocol. Moreover, because of blockchain's openness, any modification of the protocol requires the consensus of the majority of the nodes.[93] Accordingly, users do not have to trust a third party for the management of the software. This highly decentralized technology is able to affect power dynamics in the online environment since in centralized platforms the operator is able to change the network's features without asking for prior consent from its users. In this sense, blockchain provides users with more autonomy and control over the platforms' activities and processing of data.

Encryption and pseudonimity. Despite the transparency of the ledger, the combination of end-to-end encryption of the communication requiring private and public keys together with pseudonimity can mitigate the privacy concerns arising from the necessary publicity of the ledger.

4.2 Blockchain and the loss of individuals' control

[92] Benkler, Y. (2016) "Degrees of Freedom, Dimensions of Power" 145(1), p. 32.

[93] However, while in a (permissionless) blockchain the operations of the code are public, the code source may be not.

If, on one hand, blockchain can be a privacy-enhancing technology, on the other hand it can be problematic for its users' privacy because of the irreversibility of the ledger, its transparency, pseudonimity and possible application of blockchain analytics.

Irreversibility. As seen in *Chapter II*, blockchain can have several different applications. It can be used to register certificates, to engage in economic transactions, to order medical prescriptions and so on.[94] Therefore, blockchain can record data that someone may have a legitimate interest in having it altered or deleted. This could be data that at the time of the transaction was not of a particular concern but that can become so later on. For instance, someone can have an interest in deleting or modifying the personal address in case of someone's abuse, as well as the gender registered in case of transition to a new one, or the information relating to personal insolvency after long time from that event, the sensitive data relating to children, and much more. In order to have data removed, half of the nodes would have to cooperate to rebuild the chain of blocks since data were added. However, meanwhile this time-consuming operation is carried out, new transactions cannot be validated.[95] The loss of individuals' control over their personal data in this case is caused by the impossibility or high difficulty in the exercise of individuals' rights to rectification and erasure (right to be forgotten).

Transparency. As already pointed out, coordination without a central actor requires the nodes to check the validity of the transactions. In order to do so they access to all the previous transactions relating to the parties involved. In other words, each node needs to trace the full financial history of the actors of a transaction. Such visibility of all the interactions occurred in the blockchain can be highly intrusive for the privacy of the individuals involved, even more considering that public blockchain are open to anyone in the world. The individuals' interactions in the blockchain are visible to thousands of participants and such circumstance risks to clash with the principles of data minimization and storage limitation.

Encryption and pseudonimity. Even though pseudonyms are used to protect the users' identity and encryption techniques are employed to protect the content of the communication, metadata remain visible in the public ledger allowing to trace the operations carried out by the user.

Transparency of metadata, identifiability of the users and immutability of the chain can represent a dangerous mixture for the users' privacy and protection of personal data when data analytics can be applied. Specific tools have been developed in order to associate Bitcoins' pseudonyms with corresponding real identities and to retroactively rebuild the entire history of users' transactions to and from one specific address, the movements in and out of a wallet and from wallet to wallet. Indeed, profiting from the pseudonymous nature of Bitcoin, this first application of blockchain has also been used for criminal purposes (i. e. money laundering), although not prevalently. To oppose illicit activities in the Bitcoin, specific data analytics techniques have been developed in order to attribute the entire transaction history to an identifiable person and check whether he or she is linked to criminal activities. This means that through blockchain analytics the mass monitoring of blockchain's transactions is possible, for example, the Bitcoin's ones. Therefore, following this analysis, bitcoin

[94] The Estonian government is using blockchain to enable citizens to use their ID cards for several services: to order medical prescriptions, vote, apply for benefits, pay taxes, to review permits, etc. Look at: https://e-estonia.com.

[95] Open Data Institute – ODI (2016) "Applying blockchain technology in global data", Techinical Report, p. 17.

tagged because of their link with illegal services or goods could be rejected when employed for a transaction. Consequently, even those who have marginal association of their public key with a criminal identity may encounter refusal from financial or commercial operators to engage in transactions.[96] Therefore, this combination of weak pseudonomity together with the transparency of the ledger can even foster the opacity relating to how decisions having legal effects on individuals' lives are taken, risking to increase exclusion, discrimination and the loss of self-determination capabilities.[97]

Other concerns for the individuals' control: algorithmic governance. The mixture of huge amount of data shared in the network, developments in data mining techniques and the application of "smart contracts" is seen as capable of creating a new normative system built upon algorithms. A new digital common law is even advanced by scholars, assuming that a community of a network's users can give rise to a new rule of law characterized by algorithms and self-execution.[98] Algorithmic contracts are deemed to increase in business-to-business as well as in business-to-consumer transactions. Algorithms, from mere tools for the execution of contracts may gain a more central role when these become self-learning (machine-learning). Given certain objectives and parameters, the algorithms acting as an agent, will process the output through a process that the creator of the smart contract may not even understand. Smart contracts on the Ethereum present a higher level of automation compared to other algorithmic contracts.[99] As mentioned in *Chapter II*, smart contracts can create decentralized autonomous organizations (DAO) that once bounded to each other do not need a traditional business entity as a central decision-maker. The decisional process indeed can be directly encoded. To its extremes, decentralized autonomous organizations may lead to the loss of control by its members. Though more automation means optimization of services, on the other one it lessens individuals' autonomy fostering the black-box society.[100]

4.3 Blockchain and the GDPR

The blockchain's privacy risks considered in the previous paragraph affect principles and rights recognized and protected by the European data protection law, especially through the last piece of legislation approved on this matter: the General Data Protection Regulation or GDPR (Reg. EU 2016/679). European data protection law finds application since personal data are processed and stored in blockchain. Indeed, as already mentioned, the lack of a central trusted party requires as a counterbalance a high level of coordination among peers of the network, which is achievable making

[96] To name some of the companies developing blockchain analytics: Coinanalytics, Elliptic, Coinometics, etc.

[97] These critical aspects are also dealt with in UK Government Office for Science "A Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser", pp. 50-51

[98] Clippinger, J. H., Bollier, D. (2012) "The Rise of Digital Common Law An Argument for Trust Frameworks: Digital Common Law and Digital Forms of Governance", ID3.

[99] Other algorithmic contracts are: high frequency trading (HFT) of financial products; dynamic pricing that sets prices based on market information. See: Henry Scholz, L. H. (2016) "Algorithmic Contracts", Stanford Technology Law Review. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2747701.

[100] Wright, A., De Filippi, P. (2016) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia."

data available to the participants through a distributed and public ledger. Although users' identity is covered by pseudonyms and the content of the communication is encrypted, the transparency of the ledger requires at least the publication of the addresses of the subjects involved in the communication flow, the length of time and the type of transaction. In other words, to be made available are the metadata, which can also be personal data. Indeed, according to Art. 4 of the GDPR, "*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 […].*" In addition, Recital 26 sets forth that "*data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*." Therefore, pseudonimity only makes it harder to identify the data subject, but not impossible.[101] It follows that the information shared in the blockchain qualifies as personal data and, therefore, the GDPR applies. The main blockchain's controversial aspects with regard to the GDPR encompass:

a) the principle of accountability
b) the principle of data minimization;
c) the principle of storage limitation;
d) the right to erasure;
e) the principles of privacy-by-design and by-default;

a) Blockchain challenges the European data protection law at its very foundations. Blockchain is a peer-to-peer technology with a distributed community and fragmented actions, while the GDPR's obligations are conceived for centralized architectures where there is a clear distribution of roles and activities. In particular, under the GDPR's approach, data controllers and data processors are those actors who have to comply with this legislative framework, bearing responsibilities in case they do not. However, blockchain is a technology whose core aspect is the absence of a middleman, namely a controller. Peer-to-peer design challenges the application of traditional legal regulation and questions who must comply with the GDPR and, thus, who has to be held liable for the processing and protection of personal data through the implementation of adequate technical and organizational measures as the principle of accountability calls for (Art. 5(2), GDPR).[102]
   Nonetheless, in blockchain there is already a tendency to centralization as can be noticed in the Bitcoin network and decentralized platforms. What emerges in Bitcoin is that even if the community is entitled to participate, the effective decision-making process is in the hands of few people.[103] Moreover, miners are grouped in centralized communication pools, three of

[101] EDPS – European Data Protection Supervisor (2014), Opinion 05/2014 on Anonymisation Techniques, pp. 3, 20.

[102] On the need to integrate peer-to-peer design principle for the law: De Rosnay, M., D. (2014) "Peer-To-Peer Law: Distribution as a Design Principle for Law", Media@LSE.

[103] On the Bitcoin Improvement Proposals (BIPs) the core developers have stated that: "*We are fairly liberal with approving BIPs, and try not to be too involved in decision making on behalf of the community. The exception is in very rare cases of dispute resolution when a decision is contentious and cannot be agreed upon. In those cases, the conservative option will always be preferred. Having a BIP here does not make it a formally accepted standard until its status becomes Active. For a BIP to become Active requires the mutual consent of the community. Those proposing*

which control over 50% of the hash rate, while six pools control the 75% and the biggest individual pool the 21.3%.[104] Though being an open source project, in public bockchain only a small number of participants have the technical expertise to value eventual changes proposal. It is claimed that in case of extended adoption of blockchain services new oligarchies would be created in favour of those with technical skills since the openness of the software is not followed by equal knowledge and opportunities.[105] It follows that decentralization through blockchain may at the end only hide new forms of authority that lack of legitimacy.

b) Due both to the appended-only characteristic of the blockchain and the distributed storage of a full copy of data-sets by the computers of the the amount of personal data shared in the blockchain can only increase block after block. As well, the distributed coordination system creates a redundancy of data that may generate a tension with the principle of data minimization, which requires data to be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (Art. 5(c), GDPR). In blockchain, as already pointed out, in order to have transactions validated it is necessary to have their records distributed and stored by each participant. Stretching the meaning of this principle to the point of considering the need of each member of the network to have a copy of these data for the purposes of the processing could make this principle vain, especially when sensitive data that need special protection are concerned.

c) The perpetual storage of data in blockchain can be hardly reconciled with the principle of storage limitation according to which personal data shall be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*." Controversial is whether the purpose to be considered should be limited to the transaction in itself or, more broadly, should encompass the correct functioning of the peer-to-peer blockchain system for which immutability and therefore undetermined storage is necessary. In the second case, the principle of storage limitation would be stretched to the point of justifying perpetual storage, being this necessary to create a trustless system without a third controlling party.

---

changes should consider that ultimately consent may rest with the consensus of the Bitcoin users". Available at: https://github.com/bitcoin/bips/blob/master/README.mediawiki ; Also: "*decisions are made—or executed at least—by a team of core developers because only they have the technical permissions to accept submissions. Those core developers form, at least at first sight, Bitcoin's governance group in a narrower sense. Every adjustment to Bitcoin's governance structure must pass through the bottleneck of this small group of people*" in Gasser, U., Budish, R., West, S. M. (2015) "Multistakeholder as Governance Groups: Observations from Case Studies", Berkman Center Research Publication No. 2015-1, p. 8.

[104] "Bitcoin Mining Pool", BitcoinChain.com, 16 March 2017; Franco, E. (Feb 6 2015) "Inside the Chinese Bitcoin Mine That's Grossing $ 1.5M a Month". Available at: https://motherboard.vice.com/en_us/article/qkvxk3/chinas-biggest-secret-bitcoin-mine

[105] Atzori, M. (2015) "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" Available at SSRN: https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713

d) An alteration of the information stored in the ledger may be necessary for those individuals involved for accuracy or more privacy-related reasons. For instance, when information relating to insolvency, change of gender or name are concerned, and more.[106] Despite this need, the exercise of the rights *to rectification* (Art. 16, GDPR) and the right to *erasure* (also "right to be forgotten", Art. 17, GDPR) of personal data finds obstacles in the blockchain's technical features. The immutability of the ledger is one of the main characteristics of blockchain and while other blockchain's features can be slightly lessened, this one cannot. Even if past transactions could hypothetically be removed, this operation would need the cooperation of the 51% of the nodes for each transaction, entailing the verification of the validity of the previously affected transactions and the reconstruction of the following one, which would require the block of the activities in the blockchain.

e) There is a tension between public blockchain and principles of privacy by-design and by-default. As already pointed out, in blockchain there are security measures providing data security (i.e. encryption) but, at the same time, perpetual distributed storage, the possibility to associate pseudonyms to individuals, the lack of special and more protected processing for sensitive data, and the lack of an accountable third party for the fulfilment of individuals' claims highly challenge these principles.

4.4 The right to be forgotten and the Manni case

"*The irreversibility and transparency of public blockchains mean they are probably unsuitable for personal data*."[107]

In blockchain, the difficulties in the erasure of personal data are even more exacerbated due to the immutability of data recorded in the ledger. If in centralized architecture the implementation of the right to be forgotten is already problematic, in the blockchain it is almost impossible to be achieved. Moreover, in addition to the appended-only technical feature characterizing blockchain, there are also other kinds of concerns that should be taken into account. Indeed, in addition to the technical limits to the implementation of the right to be forgotten in the blockchain, there may be others of economic nature. The right to be forgotten is not an absolute one and need to be balanced against other interests, such as the interest of third parties in conducting business. Exemplary on this regard is the recent ruling of the European Court of Justice, Case C-398/15 *Manni* (9 March 2017). This case refers to a company public register and though the existence of significant differences with blockchain such as the immutability, it can offer interesting reflections when dealing with public blockchain. The original plaintiff, Mr Manni, requested the defendant, the Commercial Chamber of Lecce, to either erase, block or anonymize his name from the public Company Register where information about his bankruptcy was recorded. He claimed that, due to the re-use of this publicly available information in the commercial register by data brokers, his commercial reputation was prejudiced with detriment for

[106] Korenhof, P., Koops, B. J. (2013) "Gender Identity and Privacy: Could a Right To Be Forgotten Help ~~Andrew~~ Agnes Online?", in TILT Law & Technology Working Paper No. 3/2013.

[107] Open Data Institute – ODI (2016) "Applying blockchain technology in global data", Techinical Report, p. 16.

his new business. The case escalated to the Italian Supreme Court (Corte Suprema di Cassazione), which finally requested the Court of Justice of the European Union (CJEU) for a preliminary ruling. It asked whether the Directive 95/46/EC on personal data protection and Directive 68/151/EEC (amended by the Directive 2003/58/EC) on disclosure of company documents allow limits to the access of personal data in commercial registries. While the original plaintiff's claim was about the erasure, blocking or anonymization of the information concerned, the questions asked to the CJEU referred to the restriction to data availability.

Balancing the public interest in the legal certainty in trade and transparency of business information with the fundamental rights of the persons to respect for private life and protection of personal data, the Court concludes that the interference with the second one is not disproportionate when it concerns a limited amount of personal data held in the company register. Indeed, their disclosure functions as a safeguard for third parties engaging in trade. Besides, the Court added that when a long time has passed from the dissolution of a company, Member States can allow the restriction of access to data by third parties as an exception to be decided on a case-by-case basis. The relevance of the public interest in the legal certainty in trade and transparency of business information affirmed in this ruling can be used to foster some considerations with regard to blockchain, even though the two ledgers present differences. In blockchain, transactions among strangers are totally based on trust generated by cryptography and distribution of the ledger, measures that assure the validity of transactions in such a way that there is no need of a trusted third party and that the records cannot be tampered in any way. Thanks to this technology almost all kinds of financial, legal and product information can be put on such distributed public registry. Being the immutability of records the new basis of trust when a third authority is not involved, the appended-only characteristic becomes essential to conduct business in the blockchain. It follows that the interest in the legal certainty in trade and transparency of business information in blockchain finds its safeguard in the immutability of the ledger. Moreover, the amount of data collected per each transaction is limited to pseudonyms, type and length of the transaction, which may not constitute a significant amount of data unless considered together with the other transactions carried out. In the hypothetical, but highly possible, case of future mass adoption of this technology in a wide range of fields (as noted in *Chapter II*), the prevailing interest in the well-functioning of the market in the absence of a third controlling party may become the standard, with detriment for the individuals' right to be forgotten. Indeed, the integrity of the ledger, which is necessary to generate trust and legal certainty among the peers, is paramount to preserve the accuracy and publicity of the ledger. According to the interpretation of the Court, the restriction to data would still be possible in some cases. Considering blockchain technology, the possibility to limit the access to the personal data stored only to certain authorized participants would also be questionable: the reduction activity would require a central controlling entity in order to either give or not permission for the restriction. However, as it has already been stressed in this work, by-design, public blockchain is a peer-to-peer networks that rejects the presence of a central entity having control over the network.[108] The implementation of the right to reduction of data processing as an alternative to the deletion of data may therefore still be highly controversial due to the lack of a central actor able to fulfill such requests. As an alternative to the deletion of data, anonymization techniques could be

[108] Despite the peer-to-peer nature of the network, problems exist in the governance of blockchain. See: De Filippi, P., Loveluck, B. (2016) "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure", Internet Policy Review, Vol. 5, Issue 4. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852691.

implemented, although full anonimization is highly controversial as the debate over the possibility of re-identification of individuals from anonymized data reveals.[109]

4.5 Conclusion

What emerges from the main points highlighted in this work is that at the current state of the art public blockchain services do not comply with the recently updated European data protection law and risk to make individuals even more vulnerable instead of empowered, notwithstanding the step forwards taken by the new GDPR towards the provision of more individuals' control over their personal data. Immutability, transparency and distribution are therefore critical features if not combined with appropriate safeguards. Moreover, blockchain's governance is highly controversial due to centralization tendencies that can give rise to new forms of unofficial elites having control over the system but lacking of legitimacy. If not regulated, blockchain may replicate what has happened with the Internet that from a decentralized space has turned into a centralized one in the hands of powerful corporations. At its worst, it could become a new version of the panoptic, a distributed one where the controllers are those who know the code. Finally, users are not put in the condition to self-determine themselves due to immutability and transparency of the ledger, as well as the lack of participation in the decision-making process due to the deficiency of a highly specialized technical knowledge required for taking decisions relating to the software development. Moreover, the lack of a central party makes the exercise of individuals' rights problematic because no one is in charge of the fulfilment of these requests and decisions can be hard to be reached as the Bitcoin case has showed.

[109] Narayanan, A., Shmatikov, V. (2008) "Robust De-anonymization of Large Sparse Datasets", The University of Texas at Austin; Narayanan, A., Shmatikov, V. (2014) "How To Break Anonymity of the Netflix Prize Dataset". Available at: https://arxiv.org/abs/cs/0610105.

CHAPTER V

Conclusion

This research has meant to highlight the main benefits and concerns arising by blockchain technology from a privacy and data protection point of view. More specifically, this analysis has been carried out taking into account what is considered the core of the right to data protection to which also the GDPR is aiming at: the individuals' control over their personal data. As specified in *Chapter III*, the individuals' control over their personal data mainly encompasses, on one side, the empowerment of individuals through micro-rights to be exercised according to individuals' preferences and, on the other one, the design of technologies in such a way to allow the protection of data subjects' personal data by design and by default. In this study, it is emerged how bockchain technology may be problematic for the individuals' control over their personal data. Firstly, in this thesis, some positive factors for the users' privacy and data protection have been presented (the lack of a central entity having control over the users' personal data, the transparency on data processing and the use of pseudonimity and encryption techniques to mitigate the exposure of personal data in the public ledger). Following, problematic factors for the individuals' privacy and data protection in terms of individuals' control over their data have been highlighted. For what concerns the exercise of individuals' rights, it has been underlined how public blockchain - being a decentralized technology - lacks of a central point of control entitled to decide the processing of data and to fulfil individuals' requests, while the decentralized alternative of the consensus mechanism is difficult and slow to be achieved. Therefore, it is unclear who should be responsible for the processing of personal data and to what extent. Moreover, due to the distributed nature of the ledger, this technology may contrast with the principle of data minimization because of the redundancy of data as their copy is owned by each participant. As well, the immutability of the ledger is not in line with the principle of storage limitation since this storage is perpetual. Consequently, the right to be forgotten is also seriously challenged. Considering these main factors, blockchain's architecture is deemed not totally in line with the principles of privacy by design and by default. In particular, to constitute a high concern in public blockchain is the potentially everlasting recording of online transactions in the ledger. To have data deleted is an expression of the right to self-determination, a right that - based on the recognition and promotion of human dignity - allows the individuals' freedom to pursue the development of their own personality in terms of self-management of the information relating to them. Because of the importance of "being forgotten" in a world where every action taking place through the Internet leaves its fingerprint, it is a matter of fundamental relevance to be able not to be trapped and judged so strictly by one's own past, a condition that can foster the categorization of society and its control. As it has been highlighted in this study, informational control is important for identity-building and privacy but knowing that every action may be permanently stored may also have a chilling effect on someone's freedom to interact in the virtual space. Indeed, privacy is also functional to the exercise of other rights and freedoms. Besides, the possibility of the immutability combined with blockchain analytics is of high concern for the possibilities of digital surveillance.

It appears that GDPR and current public blockchain - both promising the empowerment of individuals - clash with each other. On one side, there is the central architectural model whose privacy risks can be tempered with the implementation of the General Data Protection Regulation that introduces new

obligations for data controllers and processors. On the other one, there is the decentralized architectural model represented by blockchain, where the novelties introduced by the new Regulation in order to give more control to individuals cannot take place due to its decentralized architecture. Accordingly, the brand new GDPR - which is not even yet directly applicable and promises to be technological neutral - is already gravely challenged by this new technology.[110] If the reason behind the need for more decentralization in the web is to have more control over one's fingerprint, the result offered by blockchain may not represent a better alternative. Immutability of the information recorded in such ledger risks to become a permanent trap from which it is hard to get out. Decentralization is therefore not in itself the solution for privacy and data protection. Moreover, such decentralization is not even effective due to the presence of a tendency towards centralization in blockchain that risks to give rise of unofficial new oligarchies.

Based on the aforementioned considerations, it is deemed that public blockchain – taking into account the current state of the art – makes it hard for the European data protection legislation to be applied and, therefore, for the individuals' control to be exercised. With this, it is not meant to say that blockchain is an obstacle for the privacy and the data protection of the individuals. This technology is still at an early stage and from month to month advancements are done in terms of new fields of applications, as well as of new privacy measures. There are fields in which blockchain do not have a privacy impact for the individuals such as the recording of product's supply chains, patent and public services and where it can bring more efficiency or in case permissioned and private blockchain are involved. Therefore, it may be reasonable to restrict the application of this technology to those fields that do not have an alarming impact on the users' privacy.

To conclude, an effective individuals' control over their personal data requires the concrete possibility for data subjects to exercise their rights and for principles to be applied, a result that is not necessarily linked to the system's architecture. A centralized architecture compliant with data protection principles and rights could be a better solution when compliant with European data protection law than a decentralized one with a privacy-hostile design that leaves the individuals unprotected and in the hands of techno-elites where power dynamics are blurred. Therefore, the development of blockchain should not be barely left to techno regulation and law regulators should better address the problems for the privacy and data protection of its users in order to let develop a privacy-friendly blockchain technology where data protection principles can find application.

[110] On the GDPR's technological neutrality, look at European Commission – Statement, "Joint Statement on the final adoption of the new EU rules for personal data protection", Brussels, 14 April 2016. Available at: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm.

Bibliography

Allen, D. (2011) "The Institutional Revolution: measurement and the economic emergence of the modern world", University of Chicago Press.

AM Eastern Daylight Time, "GovCoin Systems Implements Social Welfare Payments Distribution Trial for UK's Department for Work and Pensions", 7 July 2016. Available at: http://www.businesswire.com/news/home/20160707005803/en/GovCoin-Systems-Implements-Social-Welfare-Payments-Distribution

Article 29 Data Protection Working Party (2016), "Guidelines on the right to data portability".

Ascribe. Available at: https://www.ascribe.io.

Atzori, M. (2015) "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" Available at SSRN: https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713

Barlow, J. P (1996) "A Declaration of the Independence of Cyberspace". Available at: https://www.eff.org/it/cyberspace-independence.

Basic Law for the Federal Republic of Germany. Available at: https://www.btg-bestellservice.de/pdf/80201000.pdf.

Benkler, Y. (2016) "Degrees of Freedom, Dimensions of Power", Daedalus 145(1), 18-32.

Berberich, M., Steiner, M., (2017) "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?", 2 Eur. Data Prot. L. Rev., 422.

Birnhack, M. D. (2011) "A Quest for A Theory of Privacy: Context and Control", Jurimetrics, Vol. 51, No. 4.

BitLand. Available at: http://landing.bitland.world .

Bitstamp. Available at: https://www.bitstamp.net.

BlockchainNews, "Blockchain Startup Bitland to Implement Blockchain Property Records in Ghana", 19 May 2016. Available at: http://www.the-blockchain.com/2016/05/19/blockchain-startup-bitland-to-implement-blockchain-property-records-in-ghana/ .

Bozic, N., Pujolle, G., Secci, St. (2016) "A tutorial on blockchain and applications to secure network control-planes", Smart Cloud Networks & Systems.

Buitelaar, J.C. (2012) "Privacy: Back to the Roots", German Law Journal, 13/3, 171-202.

Buterin, V. (2014) "Ethereum: A next-generation smart contract and decentralized application platform" Available at: https://github.com/ethereum/wiki/wiki/White-Paper.

Buterin, V. (August 7th, 2015) "On Public and Private Bockchain". Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Buterin, V., et al. (2016) "A Next Generation Smart Contract and Decentralized Application Platform", Ethereum White Paper, Available at: https://github.com/ethereum/wiki/wiki/White-Paper.

BVerfGE 65,1 – Volkszählung.

Castells, M. (2001) "The Internet Galaxy: Reflections on the Internet", Business and Society, Oxford University Press, Inc. New York.

CFP: Blockchain Applications in Artificial Intelligence And Cognitive Science, 6 April 2016. Available at: http://www.coindesk.com/ibm-watson-artificial-intelligence-blockchain/

Charter of Fundamental Rights of the European Union, 2000/C 364/01. Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Clarke, R. (1994) "Dataveillance by Governments: The Technique of Computer Matching", Information Technology & People, Vol. 7 Issue: 2.

Clippinger, J. H., Bollier, D. (2012) "The Rise of Digital Common Law An Argument for Trust Frameworks: Digital Common Law and Digital Forms of Governance, ID3.

CoinDesk, "Ethereum Launches Long-Awaited Decentralized App Network", 30 July 2015, http://www.coindesk.com/ethereum-decentralized-app-network-launch/

Commissioner Kuneva, Roundtable on Online Data Collection, Targeting and Profiling, 31 March 2009, http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committe and the Committes of the Regions, "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21th Century, COM(2012) 9 final, Brussels, 25.01.2012.

Conoscenti, M., et al (2016) "Blockchain for the Internet of Things: A Systematic Literature Review", The 3rd International Symposium on Internet of Things: Systems, Management and Security, Agadir (MAR).

"The Crypto Anarchist Manifesto" (1988), Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html –

"Cypherpunk's Manifeto" (1993). Available at: https://www.activism.net/cypherpunk/manifesto.html.

De Filippi, P., Loveluck, B. (2016) "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure", Internet Policy Review, Vol. 5, Issue 4. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852691.

De Rosnay, M., D. (2014) "Peer-To-Peer Law: Distribution as a Design Principle for Law", Media@LSE.

De Terwangne, C. (2013) "The Right to be Forgotten and the Informational Autonomy in the Digital Environment", European Commission Joint Research Centre.

del Castillo, M. "IBM Watson is Working to Bring AI to the Blockchain", CoinDesk, 5 April 2016, http://www.coindesk.com/ibm-watson-artificial-intelligence-blockchain/ .

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W. (2011) "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements", Requirements Engineering, Springer, Volume 16, Issue 1, Special Issue on Digital Privacy.

Dingledine, R., Mathewson, N., Syverson, P. (2004) "Tor: The second-generation onion router", 13th USENIX Security Symposium.

Dix, A. (2011) In "Bundesdatenschutzgesetz", edited by S. Simitis, 1207–1487. Baden-Baden: Germany: Nomos.

EBA Working Group on Electronic and Alternative Payments (2015)"Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios. An exploration for transaction banking and payments professionals".

ECtHR, *Evans v. United-Kingdom*, 7 March 2006, req. N. 6339/05 with the wording of "a right to personal autonomy."

EDPS – European Data Protection Supervisor (2014), Opinion 05/2014, "EDPS Opinion on Anonymisation Techniques". Available at: https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf.

EDPS - European Data Protection Supervisor (2015), Opinion 7/2015, "Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability. Available at: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

EDPS - European Data Protection Supervisor (2016), Opinion 9/2016, "EDPS Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data". Available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

EDPS - European Data Protection Supervisor (2016), Opinion 9/2016, "EDPS Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data". Available at: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

EPRS – European Parliamentary (Feb. 2017) "How blockchain technology could change our lives."

EPRS – European Parliamentary Research Service (Febr. 2017) "How blockchain technology could change our lives."

EPRS – European Parliamentary Research Service (Febr. 2017) "How blockchain technology could change our lives".

European Commission – Statement, "Joint Statement on the final adoption of the new EU rules for personal data protection", Brussels, 14 April 2016. Available at: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm.

European Commission, "Take control of personal data". Available at: http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf.

Filipovikj, P., & Holmstedt, C. (2012) "Comparison between centralised and decentralised systems and how they cope with different threats", Abgerunfen am, 22(08).

Fischer-Hubner, S., Hoofnagle, C., Krontiris, I., Rannenberg, K., Waidner, M. (2011) "Online Privacy: Towards Informational Self-Determination on the Internet", Dagstuhl Manifestos, Vol. 1, Issue 1, pp. 1-20. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468200.

Foucault, M. (1977) "Discipline and punish: the birth of the prison", Pantheon Books: New York.

Franco, E. (Feb 6 2015) "Inside the Chinese Bitcoin Mine That's Grossing $ 1.5M a Month". Available at: https://motherboard.vice.com/en_us/article/qkvxk3/chinas-biggest-secret-bitcoin-mine

Fuchs, O., (2011), "Towards an alternative concept of privacy", JICES, Vol. 9, No. 4.

Galic, M., Timan, T., Koops, B. J. (2016) "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation", Tilburg Law School Research Paper No. 13/2016.

Gasser, U., Budish, R., West, S. M. (2015) "Multistakeholder as Governance Groups: Observations from Case Studies", Berkman Center Research Publication No. 2015-1

Goel, V., "Facebok tinkers with users' emotions in news feed experiment, stirring outcry", The New York Times, 29 June 2014. Available at: https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html?_r=0 .

Goldsmith, J., Wu, T. (2006) "Who Controls the Internet: Illusions of a Borderless World", New York: Oxford University Press.

Google Spain, Case C-131/12, p. 94. Available at: http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

Gordon, D. (1997) "The electronic panopticon: a case study of the development of the national crime records system", Politics and Society, 15(4): 483-511.

Gutwirth, S., et al. (2010), "Data Protection in a Profiled World", Springer: Dordrecht.

Henry Scholz, L. H. (2016) “Algorithmic Contracts”, Stanford Technology Law Review. Available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2747701.

https://ethereum.stackexchange.com/questions/2464/what-does-it-mean-that-ethereum-is-turing-complete.

Hughes, E. (1993) “A Cypherpunk’s Manifesto”, https://www.activism.net/cypherpunk/manifesto.html.

Hustinx, P. (2005) “Data Protection int he European Union”, Privacy & Informatie.

Hustinx, P. (2010) “Privacy by design: delivering promises”, in Identity in the Information Society, Volume 3, Issue 2, pp. 253-255.

Information and Privacy Commissioner, Ontario (Canada) and Registratiekamer (Netherlands), Privacy-Enhancing Technologies: The Path to Anonymity (Volume I), 1st August 1995. Available at: http://tinyurl.com/yenjgns.

Koops, B. J. (2014), “The trouble with European data protection law”, International Data Privacy Law, doi: 10.1093/idpl/ipu023.

Korenhof, P., Koops, B. J. (2013) “Gender Identity and Privacy: Could a Right To Be Forgotten Help ~~Andrew~~ Agnes Online?”, in TILT Law & Technology Working Paper No. 3/2013.

Lampert, L., et al., (1982) “The Byzantine General Problem”, 4 ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS, p. 382.

Lazaro, C., Le Metayer, D. (2015) “The control over personal data: True remedy or fairy tale?” ScriptEd, Vol. 12, Issue 1.

Lessig, L. (2006) “Code and Other Laws of the Cyberspace”, New York: Basic Books.

Lynskey, O. (2015) “Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez”, Modern Law Review, 78(3), pp. 523-534. Available at: http://eprints.lse.ac.uk/61944/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Lynskey%2C%20O_Control%20personal%20data_Lynskey_Control%20personal%20data_2015.pdf.

Maxwell, W. J., Bourreau, M. (2015) “Technology Neutrality in Internet, Telecoms and Data Protection Regulation”, in Computer and Telecommunications Law Review.

McKie, S., “The Blockchain Meets Big Data and Realtime Analysis”, Bitcoin Magazine, https://bitcoinmagazine.com/articles/blockchain-meets-big-data-realtime-analysis-1435183048/.

Moerel, E. M. L. (2014), “Big data protection: How to make the draft EU Regulation on Data Protection Future Proof”, Tilburg: Tilburg university. Available at: https://pure.uvt.nl/portal/files/2837675/oratie_Lokke_Moerel.pdf.

Moerel, L., Corien, P. (2016) “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”. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123.

Monopolkomission Report, “Competition policy: The challenge of digital markets”, 2015, p. 36.

Moschandreas, M. (1997) “The Role of Opportunism in Transaction Cost Economics”, in Journal of Economic Issues, Vol. 31, No. 1, pp. 39-57.

Nakamoto, S. (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System”. Available at: https://bitcoin.org/bitcoin.pdf.

Nakamoto, S. (2009) “Bitcoin Open Source Implementation of P2P Currency”, P2P FOUNDATION. Available at: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source .

Nakamoto, S. (2010) “Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG.” Bitcointalk. Available at: https:// bitcointalk.org/ index.php.

Narayanan, A., Barocas, S., Toubiana, V., Nissenbaum, H., Boneh, D. (2012) “A Critical Look at Decentralized Personal Data Architectures”, Cornell University, New York.

Narayanan, A., Shmatikov, V. (2008) “Robust De-anonymization of Large Sparse Datasets”, The University of Texas at Austin.

Nussbaum, F. (1933) “A History of the Economic Institutions of Modern Europe: An Introduction of “De Moderne Kapitalismus” of Werner Sombart”m New York: Crofts.

Open Data Institute – ODI (2016) “Applying blockchain technology in global data”, Techinical Report.

Palmer, D. (2016) “Blockchain Startup to Secure 1 Million e-Health Records in Estonia”. Available at: http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/

Pasquale, F. (2015), “The Black Box Society”, Cambridge, MA: Harvard University Press.

Peppet, S. R. (2011) “Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future”, in Northwestern U. Law Rev., Vol. 105, p. 1183.

Pilkington, M. (2015) “Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, Olleros, F. X., Zhegu, M. Elgar, E. (eds.).

Reiman, J.H. (1989) “Privacy, Intimacy, and personhood”, in *Philosophical dimensions of Privacy*, Schoeman, F.D. (ed.).

Rouvroy, A., Poullet, Y (2009), “The Right to Informational Self-Determination and the Values of Self-Development: Reassessing the Importance of Privacy for Democracy”, in: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds.) “Reinventing Data Protection?”, Springer, Dordrecht.

Rubenfeld, J. (1989) “The Right of Privacy”, 102 Harv. Law Rev., 737–807.

Rubinstein, I. S. (2012) “Big Data: the End of Privacy Or a New Beginning?”, NYU School of Law, Public Law Research Paper No. 12-56. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659.

Solove D. J. (2013), Privacy Self-Management and the Consent Paradox. In: Harvard L. Rev., Vol. 126, pp. 1880-1903.

Solove, D. J. (2009) “Book Notes: Understanding Privacy”, Osgoode Hall Law Journal 47.4.

Swan, M. (2015) “Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization)”, http://www.the-blockchain.com/docs/Blockchain%20Thinking%20-%20The%20Brain%20as%20a%20DAC%20-%20Decentralized%20Autonomous%20Organization.pdf.

Swan, M., (2015) “Blockchain: Blueprint for a New Economy”, O’Reilly Media.

Szabo, N. (1997) “The Idea of Smart Contracts”.

Szabo, N., (1994) “Smart Contracts”.

Tavani, H. T. (2007) “Philosophical theories of privacy: Implications for an adequate online privacy policy”, Metaphilosophy 38(1):1-22.

The Economist, “The promise of the blockchain. The trust machine”, 31 october 2015. Available at: http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

The UK Government Chief Scientific Adviser (2016) "Distributed Ledger Technology: beyond blockchain."Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Ubiquity. Available at: https://www.ubitquity.io/site/index.html.

Vodafone, "Vodafone Smart Summer – How the Internet of Things could make summers smarter". Available at: http://www.vodafone.com/content/index/what/technology-blog/smart-summer.html.

Weinberger, D., "How the Father of the World Wide Web Plans to Reclaim It from Facebook and Google", in Digital Trends, August 10, 2016, http://www.digitaltrends.com/web/ways-to-decentralize-the-web/ .

Westin, A. (1967) "Privacy and Freedom", Bodley Head, London.

Williamson, O. E. (1973) "Markets and hierarchies: some elementary considerations", American Economic Review 63(2): 316-25.

Williamson, O. E. (1985) "The Economic Institutions of Capitalism", New York: Free Press.

Wright, A., De Filippi, P. (2015) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia."