LUISS

Department of Law

Master of Science in Law, Digital Innovation and Sustainability

Course of Data Protection Law

Sit Tibi Web Levis - blockchain technology, digital legacy, identity, and data ownership in the online afterlife

Prof. Filiberto E. Brozzetti
SUPERVISOR

Prof. Giuseppe D'Acquisto
CO-SUPERVISOR

Giorgio Filippo Remotti
630683
CANDIDATE

Academic Year 2022/2023

Summary

More attention should be paid to the governance of digital identities and assets in the afterlife, often neglecting that, unless some measure is taken, they might live on forever uncontrolled. The legal uncertainty around afterlife data protection and the increasing popularity of online memorialization among internet users has sparked a fundamental question that has inspired the here present thesis work: *Can innovative technologies such as blockchain be applied to enhance the post-mortem protection and self-governance of digital assets and identities?*

Distributed Ledger Technologies, DLT, refers to a category of data storage architecture decentralized by design that stores information across multiple data storages called ledgers. DLT allows each transaction to be recorded, shared, and synchronized across all the nodes participating in the ledger network. The participant nodes, therefore, exchange information among themselves (Peer-to-Peer, P2P) at any time.

The distributed nature of the ledger implies that no centralized storage(s) exists; as a matter-of-fact redundancy is a key element to ensure that stored information cannot be altered or deleted arbitrarily – without the other nodes' validation, no changes can be made. Furthermore, since many copies of the "register" exist, it is also theoretically possible to have many backups of the "chain."

Blockchain is one of the many solutions falling within the wider family of DLT. As the name "blockchain" suggests, the distributed ledger is organized in an infinite sequence of blocks, each representing a transaction. The content of each block is encrypted using hashing algorithms such as SHA-256, creating a unique alphanumeric signature of the content. The block's hash constitutes one of the information available to public display together with the previous block's hash – so effectively creating a permanent link within the sequence of transactions- and the timestamp that shows when the transaction was validated. The security of the overall sequence of transactions is granted by the fact that if a block were to be altered, the entire chain would, metaphorically, fall apart since the hash functions would no longer match. This implies that each block is necessary for the existence and survival of the protocol and the therein stored digital assets.

What makes blockchain so valuable and powerful as a technology has to do, as already presented with its technological functioning while creating a secure environment built on accountability, transparency, resiliency, and decentralization as well as a personal liability – where the protocol allows to do so. In a more idealistic light, blockchain aims to deliver a secure, accountable, transparent, and tamper-proof system to store and exchange information directly among nodes. In the light of financial independence, bitcoin and the *crypto fever* have attracted conspicuous amounts of users in search of profit and users/owners of an ecosystem where monetary exchanges and value are no longer controlled nor administered by central banks. Besides the most "viral" application just presented, it is evident that blockchain has – as already said – potentially unlimited possibilities to radically innovate, shape, and create new sectors and services.

Among the possible non-financial applications, blockchain can be used in the domain of Online Identity management, allowing users to set up a Self-Sovereign Identity.

Self-sovereign identity (SSI) is the idea that individuals and businesses can keep their personal identification information on their devices. They have the freedom to select which specific details they want to share with validators without having to depend on a centralized repository of identity or data.

Within a decentralized identity framework, users assume responsibility for their security, meaning they can choose to employ their security measures or delegate this task to external entities.

The fact that virtually anything can be stored on the blockchain, i.e., personal and non-personal data, implies that GDPR compliance must be taken into account, as personal data can potentially be part of the processing. Especially considering the relationship between the GDPR and blockchain technology, it becomes immediately evident that certain rights of the data subject and the general applicability of said regulation need to be reevaluated in the light of technological and legal innovation.

As previously presented, blockchain technology leverages the permanent concatenation of transactions and their content to sustain the existence and well-functioning of the entire protocol. Hence, once they become part of the chain, data assume a structural function. The permanent availability and persistence of potential personal data imply the necessary reconsideration and applicability of certain data protection rights envisioned by the European legislator, such as the right to be forgotten. An attempt for reconciliation and "traditional" compliance achievement appears almost insolvable since the technology (blockchain) "obeys its own internal rules" colliding with external regulations.

This is especially true concerning the inability to exercise data rights such as the right to be forgotten and rectification as traditionally envisioned by the GDPR can grant, on the other hand, a new-found ground for protection and autonomous control over data and digital assets.

Decentralization poses a further ground for concern since data protection has, until now, been conceived as something applied and applicable to centralized entities. This especially complicates the identification of crucial figures, such as the controller and processor, who are usually responsible and liable for processing personal data. In a blockchain environment where a clear decisional center is only sometimes identifiable.

Together with the new-gained self-determination ability, protocol participants assume -at least theoretically-responsibility for their processing, sparking considerable difficulties from an internal governance perspective, which can still be solved through the ex-ante identification/delegation of a few selected entities to avoid unnecessary diffusion and confusion of responsibility and liability among users.

Although the regulatory landscape and the technological one need to cooperate and adapt according to their mutual needs, the effort to reconcile "what law wants and what technology is" might bring significant benefits for society, including creating a data self-governance system. In the previous chapter, a comparison has been presented between the before and after blockchain adoption where, among the many differences, an interesting phenomenon could be observed regarding the user's position in exercising powers and rights against intermediary entities.

Regulations like the GDPR find their purpose when considering providing data subjects with the necessary toolbox to create a line of defense against any potential exploitation of their data since little to no control can be exercised over them.

Blockchain ecosystems radically reshape the assumption that users lack any decisional power simply by including them into the governance system through the consensus mechanisms as well as substantial freedom to store anything inside a given block, subsequently equipping them with new powers, responsibilities, and capabilities, including personal data self-governance in the digital personal sphere.

Internet and social media have radically changed individual and collective existence by allowing anyone to continuously establish a personal narrative by creating multimedia content and said content and the voluntarily and involuntarily generated data and so their personal digital footprint. A user's digital footprint eventually becomes an extension of one's personal identity transforming it into a *digital identity* that can be understood as *a complex*, continuously self-constructed narrative system about the user. Said digital identities are, therefore, polyhedric entities formed by a different digital asset, including but not limited to personal data and multimedia content. Beyond the mere identification of a user's online presence, the digital footprint becomes an extension of one's personal identity transforming it into a *digital identity* that can be understood as *a complex*, continuously self-constructed narrative system about the user.

Albeit the non-contestable importance of said assets to ensure users can interact online, it is clear that digital identity and assets follow but do not resemble the biological lifecycle of their owners; thus, once generated and available online – if not otherwise specified- they remain within cyberspace potentially forever. The latter implies that digital identities not only survive death but also enable users to live forever in cyberspace and through their digital identity.

Logically, the innovation brought by social media has also affected how digital identities – or, more humanely said- users can be remembered after death. Online expressions of bereavement have shown that "keeping" something, albeit immaterial, but the deceased, i.e., a social profile with photos and messages, can significantly help the elaboration of grief among family and close friends. As the social practice of online grieving has expanded, further concerns have emerged about the necessity to govern the phenomenon of the online afterlife. For instance, individual social media platforms or other third-party services have envisioned profile management tools to ensure that the profiles' content – although available for display – will not be mistaken for "living profiles" or, even worse, become a target for potential misuse or other conducts affecting the dignity of the deceased. This has partly led platforms such as Facebook to incorporate the possibility of memorializing social profiles or nominating a legacy contact to execute the deceases mandate to either be memorialized or have the profile deleted. Albeit seemingly appropriate to safeguard identities and assets in the afterlife, it shall be said that memorialized profiles still suffer from a rather decreased ability of direct control by the heirs while further maintaining a considerable exposure to cyber threats such as data loss, breaches or generally any other event affecting their confidentiality, integrity, and availability.

The question of digital asset ownership and inheritance becomes crucial when considering how easy it is to fetch basic information such as name, surname, and profile picture if no safeguards are foreseen. Hypothesizing that a given profile is memorialized, all the information, contents, and that make up that digital identity of a particular user are still "owned" and controlled by the platform provider or, under the GDPR jargon, the controller.

This leaves significant room for non-addressed threats such as data breaches and possible exploitation of a particularly delicate and sensitive moment for bereaved friends and family members. Social media platforms have an intrinsic interest in "dead accounts" due to the legal uncertainty that currently affects personal data in the afterlife, making it harder for data subjects to strive for a claim of control over their digital identity and assets. An identity management system should give individuals ownership over their data, its use, distribution, or non-distribution. The blatant importance of said assets in life imply a considerable interest and necessity to ensure their protection from undue exploitation, access, or loss through legal instruments -mainly the GDPR- as well as technological products and services.

To better understand the possibility of innovating the governance of post-mortal data, and ensuring their inheritability and ownership, it is crucial first to understand the regulatory landscape addressing the issue under analysis. Albeit personal data are not protectable under the GDPR, it would be inexact to state that the digital afterlife cannot be harnessed and controlled. Conversely, its protection and governance result from a complex cross-contamination of different legal "forces." For instance, managing data and digital assets in the afterlife is often possible through the channels of inheritance law as – according to some views – albeit digital, they maintain the same status as tangible personal goods of the deceased. For personal and non-strictly personal data, some member states (Italy and France, for instance) enable the legitimate owner to express, ex-ante, a mandate to determine what shall happen with their data and assets after their death. Subsequently, to the present legal analysis, further reasoning has been dedicated to a deeper issue regarding the governance of post-mortal data and assets, which can be found in the unsolvable clash between the deceased right to be forgotten on one side and the living's right to memory. Previous analysis has assessed that contemporary society and cultural practices such as grief and bereavement are already happening online, and "keeping" something – although immaterial – about the deceased can yield significant benefits from a psychological footing.

As such, it becomes crucial to understand how this clash between digital memory and oblivion can be solved. One of the main findings of this work revolves around the assumption that a solution to the latter is possible by reconceptualizing the right to be forgotten and the act of "memorializing" in a different light and possibly through the use of technology. The traditional interpretation of the GDPR considers the right to be forgotten as a complete and irreversible process that renders data completely unavailable.

Conversely, to said interpretation, it is possible to look at the act of deletion not as a monolithic but rather dynamic entity, meaning that the deletion of data does not necessarily need to be permanent and absolute but as the permanently limited availability of the assets at stake from the public, while ensuring their existence and accessibility within a private and intimate digital space. In other words, through the reconceptualization of the right to be forgotten of the deceased, not as an absolute deletion but rather a permanently restricted data accessibility and visibility from external public interference, a new-found conception of online privacy originates: Meta-privacy.

Meta-privacy is the attempt at re-creating a self-sovereign and private digital space with analog features to the private and intimate online sphere that the user can individually control. Leveraging blockchain technology to set up a digital vault that exhibits said characteristics appears possible and compatible with the *raison d'être* of many protocols that endorse user self-sovereignty, security, and data ownership through decentralization. To further ground the assumption that an innovative application of legal and technological tools can enhance the post-mortal protection of personal data and digital assets, looking at the current trends and offerings within the digital afterlife industry highlighted a series of concerns. Memories, assets, and data are still stored and made available thanks to the intermediation of third-party service providers and their (centralized) servers. More than often said, assets are openly consultable thus, publicly displayed with low-level security measures.

A further ground for concern in an ecosystem that serves perpetual digital remembrance is found through bit rot. Bit rot is the irreversible degradation or loss of digital information when the infrastructure (the hardware and software) required to access, interpret, view, and use this information is no longer available or executable. It affects digital information and the enabling technological infrastructures, radically dimensioning the idea(s) around the default perpetual existence and availability of digital content online. Without any measures taken, or better, leaving things as-is, we are nonchalantly throwing all of our data into what could become an information black hole without realizing it. Such consideration is dangerous as it radically truncates the naive assumption that the internet cannot truly die and so the therein stored contents. Applying decentralized storage solutions under the guidance of Meta-privacy solves a series of crucial nodes and concerns residing deeply into the digital afterlife industry (DAI).

Firstly, decentralized architectures imply, at their core, that third-party mediation and centralized server dependency no longer apply, creating a self-sovereign and directly controllable digital space (*a.k.a*, a digital vault). This not only enhances, directly, the protectability and controllability of digital assets but further strengthens their resiliency and availability in the long term against Bit Rot.

Blockchain directly addresses the issue of bit rot through its main technological features: decentralized storage that enables many copies of the "chain" to exist and be restored if needed, together with the add-only tendency of blockchain environments. Secondly, the ability to restrict access and visibility through blockchain storage solutions enables users to achieve meta-privacy and direct ownership – hence control-over digital assets. For instance, a given user could still request the public deletion of their digital presence while privately maintaining a "personal" copy.

The reasoning and analysis of the state of the art and proposal for re-evaluation of data governance in the light of social needs and technological innovation have been synthesized in the creation of a theoretical and practically applicable layered data access model aimed at endeavoring data self-sovereignty, long term asset resiliency and post-mortal protection through direct ownership, selective disclosure, and availability; able to foster the creation of a concrete service proposal dedicated to afterlife digital asset management.

Keywords: *digital identity, afterlife, data protection, digital assets, blockchain technology, meta-privacy, digital heritage, digital immortality, data resiliency, memory, right to be forgotten*

Table of Contents

Introduction

One of the informal rules of the Internet is that “once something enters internet it is hardly forgotten.” Through our simple online existence and, more importantly, through social media, individual users shape their persona by self-narrating themselves to the world. As these new mass self-communication tools allow for agile creation and sharing of relevant moments and long-lasting memories, they contemporarily contribute to creating ion of our online representation and self-projection, hence digital identity. Digital Identities are polyhedric entities that originate from the unique combination of Personal and non-personal data, Social Media profiles, User Generated Contents (UGCs), or broadly anything within the digital sphere that can be retraced to a particular user. Digital identities are usually confined and detained within social media platforms as these are the main space of digitally mediated interactions; they factually exist within one or more servers that the user (owner) cannot directly control. Hence, if they are not deleted or otherwise rendered ‘unavailable,” they systematically keep on existing well-beyond biological existence. Albeit this opens up new possibilities for friends and family members to find closure by reshaping mourning and remembrance practices, the Internet’s intrinsic tendency to perpetual remembrance finds a further ground for concern and research interest when considering the broader impact perpetual digital existence can have on the deceased data rights, the management of digital assets after death, as well as the involvement of information and other assets in the carrying out of cybercrimes. More than that, the potential clash between the deceased’s right to be forgotten and the living’s will and right to remember appears almost unsolvable. A possible solution could be sought by reconsidering relevant legal frameworks governing data protection while simultaneously leveraging disruptive technologies such as blockchain to extend and enhance the safeguard and resiliency of digital assets in a self-sovereign digital environment. Long-term data resiliency becomes a further ground for concern when considering the phenomenon of bit rot, which could well be the decay and oblivion of the 21st century; how can technology sustain the creation of a digital Vellum ensuring that personal and collective digital heritages will be available to future generations? This thesis work will be articulated in six chapters. Chapter One will be dedicated to assessing and presenting blockchain technology, its features, and possible applications; Chapter Two will take set the State of the art of data protection at the European level, while Chapter Three will feature a synthesis moment to reason if and how blockchain technology can become GDPR compliant. Chapter Four will introduce the concepts of digital identity and the digital afterlife to understand how death in the online environment is addressed. Chapter Five will consider the postmortem protection of personal data and other information while conducting a comparative analysis across member States, finally presenting a new way to reconcile digital memory and oblivion. Chapter Six will finally condense the content and elements of discussion of all previous chapters by conceptualizing a layered access model able to provide adequate protection of data and digital assets from external intrusion while ensuring their time-wise resiliency independently from third-party service providers.

Chapter One: Distributed Ledger Technology and Blockchain

1.1 DLT

Distributed Ledger Technologies, DLT, refers to a category of data storage architecture decentralized by design that stores information across multiple data storages called ledgers. DLT allows for each transaction to be recorded, shared, and synchronized across all the nodes that participate to the ledger network. The participant nodes therefore exchange information among themselves (Peer-to-Peer, P2P) at any time.

The distributed nature of the ledger implies that no centralized storage(s) exists, as a matter-of-fact redundancy is a key element to ensure that stored information cannot be altered or deleted arbitrarily – without the other nodes validation no changes can be made. Furthermore, since many copies of the "register" exist it is also theoretically possible to many backups of the "chain".

The consensus mechanism is what makes it possible within DLT systems to seek a common agreement among parties that, substantially speaking do not communicate directly among themselves. The problem on consensus in DLT can be explained through a classic in scientific literature: the Byzantine Generals Problem. The Byzantine Generals Problem is a classic problem in computer science and distributed systems that deals with the challenge of coordinating actions between multiple distributed nodes in the presence of faulty or malicious nodes. It is typically framed in the context of a group of Byzantine generals who are planning to attack a common enemy. The generals, who are stationed in different locations and communicate with each other via messengers, must agree on a plan of action, such as when to attack and from which direction. However, some of the generals may be traitors who are actively working against the others. These traitors may send false messages or deliberately refuse to follow the agreed-upon plan, causing confusion and potentially leading to defeat. The challenge for the loyal generals is to produce a protocol for reaching a consensus on the plan of action that is resilient to the presence of traitors. In other words, they need to design a communication and decision-making protocol that can withstand the possibility of some of the nodes being unreliable or malicious. This problem has important practical applications in areas such as distributed computing, blockchain, and cryptography. To solve the problem, a series of solutions have been proposed, one of which is the Practical Byzantine Fault Tolerance (PBFT). PBFT is a consensus algorithm that guarantees correct system operation if the number of faulty nodes does not exceed one-third of the total number of nodes.

This algorithm employs message exchanges, voting, and verification among the nodes to agree upon the order of transactions or operations. These algorithms generally involve multiple rounds of message exchanges, voting, and verification, incorporating redundancy, error detection, and fault tolerance mechanisms to ensure the system's ability to withstand faults and maintain its integrity, security, and reliability. PBFT usually involves six phases.

1. Request: A client sends a request to the network of nodes, specifying an operation to be executed.
2. Pre-prepare: The primary node, that is selected among the participating nodes, receives the request and assigns a sequence number to it. The primary then sends a “pre-prepare” message to the other nodes, including the request and its sequence number.
3. Prepare: Upon receiving the “pre-prepare” message, the nodes verify its validity, consistency, and authenticity. If the message is deemed valid, they send a “prepare” message to all other nodes, indicating their readiness to commit the request.
4. Commit: Once a node receives a sufficient number of “prepare” messages (reaching a threshold defined by the system), it sends a commit message to all nodes, signifying that it is ready to execute the request.
5. Execution and Response: Nodes execute the request, ensuring that they arrive at the same result. After executing the request, they send a response to the client.
6. View Change: In case the primary node is suspected to be faulty or non-responsive, a view change may be initiated to select a new primary node and ensure the progress of the algorithm.

By implementing these steps and exchanging messages among the nodes, PBFT allows the distributed system to tolerate faults, ensuring that the majority of correctly functioning nodes reach a consensus on the order of requests. The algorithm guarantees safety (all correct nodes agree on the same order) and liveness (requests are eventually processed) under the assumption that the number of faulty nodes does not exceed one-third of the total. The presented characteristics make Byzantine Fault Tolerance applicable in various domains, including blockchain technology, distributed databases, consensus protocols, and decentralized systems. It plays a vital role in enabling these systems to function correctly, even in the presence of potentially malicious actors or unpredictable failures, thus ensuring the system's overall robustness and effectiveness.

Cryptography is a discipline closely related to cryptology and cryptoanalysis and uses a series of computational instruments and techniques to secure information during their transfer – thus avoiding transferring or storing them in cleartext (as-is in readable format) but rather in an intelligible way. Cryptographic algorithms rely on complex mathematical equations and codes, ensuring the encoded message's confidentiality, integrity, non-repudiation, and authentication. It should also be emphasized that DLT is not a single, well-defined technology but rather signifies a wide family of many different technologies that- albeit minor differences- share common characteristics as previously described.

DLT protocols can be designed to function in different ways, prioritizing some aspects over others to create a unique value proposal to fit certain needs as opposed to others. Ultimately, the protocol's code – the self-proclaimed technological law- shapes the technological affordances and internal governance infrastructure.

1.2 Blockchain

Blockchain is one of the many possible declinations that fall within the family of DLT. Conversely to the global trend -the core technology popularly known to be at the core of Bitcoin - was first created in the early 1990s and published by Leslie Lamport (1998), in which he described a consensus mechanism to reach a common agreement among nodes where the nodes themselves could, theoretically, be unreliable or malicious. "Rather than being a completely novel technology, a blockchain is better understood as a combination of previously existing mechanisms, such as distributed ledgers, asymmetric encryption, and Merkle trees, that were linked together to enable Bitcoin in 2009." (Finck, 2018, *pp.*2)

Satoshi Nakamoto, the pseudonym used by the unknown creator of Bitcoin, leveraged the latter concepts in his own Distributed Ledger protocol that became exceedingly popular over the last decade. The popularity of Bitcoin and the increased interest, as a consequence, for blockchain technology has to be sought in what Satoshi's innovation represents for users and their presence in cyberspace. Bitcoin presented the internet with the possibility to pay online while leaving little to no traces behind, despite the transactions being permanently stored and viewable by anyone.

As the name "blockchain" suggests, the distributed ledger is organized in an infinite sequence of blocks, each representing a transaction. The content of each block is encrypted using hashing algorithms such as SHA-256, creating a unique alphanumeric signature of the content. The hash of the block constitutes one of the information available to public display together with the previous block's hash – so effectively creating a permanent link within the sequence of transactions- and the timestamp that shows when the transaction was validated. The security of the overall sequence of transactions is granted by the fact that if a block were to be altered, the entire chain would, metaphorically, fall apart since the hash functions would no longer match.

1.2.1 Permissionless

Permissionless blockchain networks are decentralized ledger networks that do not require any authorization to join the protocol; if everyone can read, write and validate blocks, they are often open-source and freely available to anyone who wishes to download them – hence have a copy of the ledger. Since anyone has the right to publish blocks, read, and issue transactions on the blockchain, resulting in an open and distributed ownership and governance model (D' Acquisto, 2021).

The considerable degree of publicity and openness of permissionless blockchains has evident advantages, fostering collaboration and crowdsourcing, but simultaneously exposes the entire network to potential attacks by malicious nodes willing to subvert the system to their benefit.

To prevent such scenarios and ensure the security of the stored information, permissionless blockchain networks often utilize multiparty agreement or consensus mechanisms that require users to expend or maintain resources when attempting to publish blocks. These consensus mechanisms exist in two variants: Proof of Work (PoW) and Proof of Stake (PoS).

PoW requires network participants, known as miners, to solve complex mathematical puzzles to propose new blocks and add them to the blockchain. The underlying principle of PoW is that the computational effort required to solve these puzzles demonstrates a certain level of work performed by the miner. In the PoW process, miners compete against each other to solve the puzzle, utilizing significant computational power and energy resources. The first miner to solve the puzzle broadcasts their solution to the network, which is then verified by other nodes. Once the solution is verified, the miner's proposed block is appended to the blockchain, and the miner is -usually- rewarded with a predetermined amount of cryptocurrency as an incentive for their effort. The security of PoW derives from it being resource intensive as a considerable amount of energy and computational power are required to solve the mathematical puzzles. Nonetheless, this acts as an incentive for "good" nodes and a disincentive for "malicious" nodes since taking control over the protocol, and the blockchain would require the attacker to possess most of the network's computational power to modify past transactions or create fraudulent blocks. Such an attack, a 51% attack, becomes increasingly difficult and economically unfeasible as the network grows.

PoS is an alternative, more sustainable consensus mechanism in blockchain networks that addresses the energy consumption and scalability limitations associated with Proof of Wo. In PoS, block validators, or "stakers," are chosen to create new blocks based on their ownership, or stake, of the native cryptocurrency. Unlike PoW, where miners compete through computational power, PoS selects validators randomly, considering their stake as a determining factor. The stake represents the number of tokens held by the validator in the network. Validators are chosen to create blocks in a pseudo-random manner, considering factors like their stake size, age, or a combination of both.

In the process, validators are required to lock a certain amount of cryptocurrency called a "stake." This stake is at risk if the validator behaves maliciously by attempting to compromise the network's integrity. The probability of being chosen as a block creator is directly proportional to the validator's stake, incentivizing them to act honestly to preserve their stake's value.

PoS offers several advantages over PoW, including reduced energy consumption, as the consensus is reached without requiring intensive computational calculations. It also provides a higher degree of scalability, as the network's capacity to process transactions increases with the number of tokens validators hold. The abovementioned mechanisms are currently the most widespread among blockchain protocols and have peculiar benefits and faults. However, they share the same goal, or rather grounding principle, which is incentivizing virtuous behaviors among nodes -by providing incentives- and disincentivizing the presence of malicious ones through "sanctions." Hence, it not only renders the perpetration of malicious activities unprofitable, if not unsustainable but also prevents malicious users from easily subverting the system.

1.2.2 Permissioned

Permissioned blockchain networks are ones where the participation to the network, conversely to permissionless blockchains, is subjected to a pre-authorization process by a central authority that on its own can be organized as a more or less centralized system. Since only authorized users are maintaining the blockchain, it is possible to restrict reading, writing as well as the issuing of privileges. Permissioned blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to authorized individuals. Their centralized nature does not interfere with the transparency, accountability, resiliency, and redundancy of the architecture found in permissionless blockchains.

They still use consensus mechanisms as in the previous cases but since participant nodes are required to undergo an authentication process the workload and resource expenditure – mainly computational power and electricity – are significantly lower than permissionless blockchains. Once the identity of a node is "validated" it gains the necessary privileges and level of authorization to enter the blockchain network. The "trustworthiness" of the node originates from an ex-ante checking process. A further level of trust, if not security, is obtained by the fact that as an authorization is issued it can be revoked if a node should embark in non-compliant practices. This is because the establishment of one's identity is required to participate as a member of the permissioned blockchain network; those maintaining the blockchain have a level of trust with each other, since they were all authorized to publish blocks and since their authorization can be revoked if they misbehave.

Consensus models in permissioned blockchain networks are furthermore more efficient from both a computational and energy-usage point of view. Permissioned blockchain networks may also be used by organizations that need to control and protect their blockchain more tightly for organizational or business needs. Beyond trust, permissioned blockchain networks provide transparency and insight that may help better inform business decisions and provide for an enhanced strict liability of the single node in case of misbehavior. Some permissioned blockchain networks support the ability to selectively reveal transaction information about a user's identity (Selective disclosure). With this feature, some degree of privacy in transactions may be obtained. For example, it could be that the blockchain records that a transaction between two blockchain network users took place, but the actual contents of transactions are only accessible to the involved parties. Some permissioned blockchain networks require participating users to be pre-authorized to send and receive transactions, effectively abandoning the idea of complete blockchain-enabled anonymity, featuring a pseudo-anonymization of the users' identity. Being the degree of anonymity lower than in permissionless blockchain, consequently, the main disincentive to the commission of illicit conducts is the identifiability of the single node. This shows that blockchain protocol by-code are not created equal and some degree of control can be obtained over a technology that often -and wrongly- is depicted as ungovernable and uncontrollable.

1.3 Purpose and Utility

Blockchain as a technology is not tied to any sector, service, or specific product; virtually speaking, it could be applied -if not forced into anything. It is potentially omni-applicable, meaning that its application is a stand-alone technology or in synergy with other ones to create new products and services and innovate and improve existing ones. Aside from the single-case applications, the overall value of the newly created tech market has reached a global value of 1,431.54 billion UDS by 2030[1], as its potential use is crucial for the development of sectors such as cybersecurity or even the digitalization of administrative procedures[2]. This trend is confirmed by looking at the exponential growth of blockchain's projected market value worldwide, which already went from 0.96 billion USD in 2017 to 19.36 in 2023 and is set to reach 162.84 billion USD by 2027 with a growth of + 1596.25% over just ten years.[3]

What makes Blockchain so valuable and powerful as a technology has to do, as already presented with its technological functioning while creating a secure environment built on accountability, transparency, resiliency, and decentralization as well as personal liability – where the protocol allows to do so. These are all distinctive features of the blockchain protocols at large and are key-enablers in the creation of a trustless-trust based mechanism meaning that; the "trust" the nodes share among them is not built on a "blind statement" but a complex and well-established code, a set of rules and mechanisms that harness the nodes' interaction. Under a more idealistic light, the purpose of blockchain is to deliver a secure, accountable, transparent, and tamper-proof system to store and exchange information directly among nodes. In the light of financial independency, with bitcoin and the *crypto fever*, has attracted conspicuous amounts of users in search of profit as well as users/owners of an ecosystem where monetary exchanges and value are no longer controlled nor administered by central banks. Beside the most "viral" application just presented, it is evident that blockchain has – as already said – potentially unlimited possibilities to radically innovate, shape, and create new sectors and services. Among the possible non-financial applications blockchain can be used in the domain on Online Identity management allowing users to set up a Self-Sovereign Identity.

Self-sovereign identity (SSI) is the idea that individuals and businesses have the ability to keep their personal identification information on their own devices. They have the freedom to select which specific details they want to share with validators, without having to depend on a centralized repository of identity data. SSI enables the creation of identities that are not tied to nation-states, corporations, or global organizations. Within a decentralized identity framework, users assume the responsibility for their own security, meaning they can choose to employ their own security measures or delegate this task to external entities.

[1] https://www.grandviewresearch.com/press-release/global-blockchain-technology-market

[2] https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=44784&content=&content_author=

[3] https://www.statista.com/statistics/1015362/worldwide-blockchain-technology-market-size/ with personal data re-elaboration.

By utilizing blockchain technology, decentralized identity solutions compel hackers to target individual data stores, which is a costly and generally unprofitable endeavor. This concept could potentially be extended to safeguard digital assets and facilitate their transfer to beneficiaries in a secure manner. In other words what was originally theorized and programmed in the late eighties of the previous century is about to inevitably overthrow the way we conceive the intricate dynamics between technology, society, economy, and law.

1.4 Before and After Blockchain

Technological innovation is “a process of industrial change that incessantly revolutionizes the economic structure from within, incessantly destroying the old one and creating a new one” (Schumpeter, 2942, *pp.*83). Inevitably, once a disruptive technology such as blockchain enters the market it causes the whole socio-economic fabric to change; this process does not only force companies and people to evolve as new products and service do, but also affects the regulatory aspect, thus the law, to rule upon increasingly complex matters that require a deep technological understanding and long-term adaptive vision. As for innovation as a broader phenomenon where the introduction of disruptive technologies changes everything requiring to operate, among the many, a shift of paradigm that does not necessarily cancel out the past as one technology is elevated to dominant design in a given market the previous technology descends occupying a lower – less preferable – option or even a market niche.

The music industry provides in this sense a useful example to show how recording technology has evolved since the last century shifting from vinyl to CDs and finally MP3 and MP4 where the latter represents the current technological standard. Still, the presence and usage of digital formats does not cancel out CDs and Vinyl records that can still be found at record stores since a small niche is still interested in them. As in the previous example, blockchain does not cancel out every currently available technology but rather creates a fracture – a *caesura* – between old and new ones. Beyond technology also the technological governance is affected as traditional rights and frameworks are required to adapt to the ongoing technological change; effectively creating a *Before Blockchain* era (B.B) and an *After Blockchain era (*A.B) (D’ Acquisto, 2021)

1.4.1 B.B.

Blockchain finds its most crucial application in the global internet domain that, traditionally speaking, has always been characterized by a varying degree of intermediation to enable the communication flow – and so interaction - between users. Intermediation, in this specific case, must be interpreted as the activity a "middle-man entity" carries out to facilitate the exchange of information e between a sender and a receiver by providing the necessary infrastructure, tools, and usage schemes in the form of a comprehensive communication service. These services facilitate *one-to-one*, *one-to-many*, or even *many-to-many* types of exchanges, as seen in messaging apps, social media, or e-commerce services. At the same time, service providers exercise a certain degree of control over the user's ability to virtually interact with other users by exchanging information and value immaterial or material goods.

Where there is a central entity, all parties involved enter a "social contract" accepting to commit and comply with the entity's rules; this often leads to users being formally free to interact as they want, although within the boundaries of the golden cage the entity - i.e., a platform provider sets out. The internets and related services that inhabit cyberspace are, in a certain sense, affected by the centripetal forces that govern the provision and usage of said services, effectively limiting the user's ability to truly self-express its usage path without undergoing the strict control of the online gatekeepers (Gillespie, 2018) exercise.

Since platforms have reached a non-neglectable size and influence, it has become evident that the relationship between the provider (platform) and the customer (user) is affected by very deep power asymmetries that require regulatory intervention. In the "before era," there was a well-established and enforceable tendency to information confidentiality (D' Acquisto, 2021) when interacting with any service provider, enforced by laws and regulations, such as the European General Data Protection Regulation (GDPR) since gatekeepers have been over-exploiting users for their data to power their algorithms and business models that could be described as data intensive. Overall, the better part of the responsibility, both legal and not, lies with the platform provider (intermediary entity), as the latter is the sole responsible for the course of action to be adopted.

A general social media platform could, for example, autonomously change its ToS (Terms of Service) or community guidelines, substantially changing the inner workings of the platform governance without consulting - but only notifying the users about the changes to be made. The platform provider also bears the legal consequences (accountability) a given change could have in cases of non-compliance as set by law. A further requirement relevant regulation has set to limit illicit conduct in the domain of personal data is the requirement to identify the controller, the processor, the legal basis for the processing, and the legitimate interest behind the processing. Centralizing implies that the decisional center is centralized and easily broken into categories, functions, activities, and associated responsibilities.

1.4.2 A.B.

Blockchain, since its introduction, has significantly changed the way our societies conceive technology and its daily application as a broader phenomenon. A significant shift can be observed when trying to explain some of the characteristics of the after-blockchain era. It has been explained how intermediation has characterized online interactions, leading to a substantial centralization and concentration of decisional power and responsibilities that inevitably fall on the platform provider (processor). In the A.B. era, the decisional center can sometimes be very hard to identify, considering that not all blockchains are governed similarly. However, it can still be seen how each node bears more or less equal responsibilities shared with all the other nodes while also being responsible for its personal behavior. Implying that potentially speaking, users can conduct transactions among themselves – as in peer-to-peer (P2P) systems, thus not requiring third-party (inter-) mediation as in the B.B era. The afore-introduced tendency to confidentiality leaves pace to an apparently antithetic trend, which is mandatory public transparency; opposing the habit of keeping something private -secure- since no one can be trusted when dealing with (personal) data. Conversely in blockchain applications transparency is the required instrument to grant the certainty of transactions [and build trust among the nodes] (D 'Acquisto, 2021, *pp.*54). In other words, within a blockchain, while still considering the intrinsic characteristics of permissioned and permissioned architectures, "everything is (sometimes) under the eyes of everyone" (*ivi*). Overall, it can be said that the centripetal force that characterizes the B.B era is converted into a centrifugal force in the A.B era as the users start bearing more responsibility as well as decisional power. This fragmentation of the decisional center inevitably has positive as well as negative spillovers such as the certainty of transactions. The empowerment of the single node (user) as third-party intermediation is no longer a must but rather an optional service. Together with the benefits the application of blockchain brings along the shortcomings that must be addressed include the impossibility, or rather immense complexity of deleting the content of a block or transaction, the substantial as well as formal difficulties that are faced when trying to identify relevant figures and processes as required by the GDPR.

This comparative exercise shows how blockchain is already shaking the socio-economic and legal framework in the digital environment. Focusing on the regulatory framework it becomes evident that data subjects’ rights are already being affected as the protection of some rights is being enhanced while others can be hardly enforced in the same way due to the technology being itself a self-governing system where the inner functioning require specific rules to function properly. Such significant variations in the context justify and […] necessitate the intervention of the regulator, which is not (should not be) aimed at restricting the adoption of this technology, but on the contrary to promote a framework of rules for blockchain actors, and of freedoms and rights for blockchain participants so that in this technological leap all benefits are amplified, and all the disadvantages minimized. (D‘Acquisto, 2021, *pp*.54) In the next chapter the regulatory framework will be further explored as to set the required ground to assess possible course of action and regulatory dialogues to both preserve a flourishing sector and provide the necessary instruments to safeguard users’ digital rights, digital assets and memories well beyond what appears to be possible.

Chapter Two: GDPR UE 679/16

The European General Data Protection Regulation (EU 679/16) is an original example of the regulatory effort put into governing the digital landscape equipping users with the necessary tools to safeguard their personal data while – at the same time – harnessing anyone processing[4] personal data for economic purposes to comply to this particular regulation. In spite being a European Regulation, and so do pe respected and applied directly by all member states, the GDPR as a broader vision, aims at extending its influence well beyond the boundaries of the European union envisioning a comprehensive and aligned global standard safeguard for data protection.

2.1 Risk based approach.

> Under the GDPR, the risk-based approach to data protection entails the obligation of the data controllers to assess the risks of data processing to the rights and freedoms of natural persons throughout every stage of the data life cycle (collection, storage, processing, retention, sharing and disposal). To fulfil its duties the data controller is expected to evaluate the likelihood and severity of risks for individual rights in the light of the nature, the scope, the context, and the purposes of the processing. (Gonçalves, 2020, *pp*.142)

This constitutes a novelty in approaching the matter of compliance if compared to the previous approach adopted by directive 95 which, in an almost utopistic way, tried to envision every possible processing scenario in order to harness it. In this sense the GDPR appears to be more flexible and adaptive, thus able to deal with the complexity and incessant innovation process the ICT are characterized by.

Overall, the risk-based approach shifts most of the responsibility on the processor and controller leaving them to determine how and through which means a given service shall be compliant with the requirements set out by law. The latter constitutes another key principle and novelty set out by the GDPR which is summarized in the concept of Privacy by design.

[4] Art.4 para. 2 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Privacy by design shifts the risk prevention and management activity from a solely policy-centric and legal perspective towards a more holistic vision that entails the involvement of both legal [guidance] and programming activity – hence coding. Art. 25 (1) states that

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, 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, […] designed to implement data-protection principles, […] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

As such a given service that requires the processing of personal data must, from its very core – its code – respect the principles and requirements set out in art.5.

2.2 GDPR Art.5

As presented, the GDPR's scaffolding is based on principles rather than explicit obligations set out by law found in Art.5 of the same regulation. Concerning the processing activity, the said activity must be lawful, fair, and transparent toward the data subject. Furthermore, data cannot be gathered and used for unlimited processing operations since, upon gathering data, the controller is required to inform the data subject about the intended purpose. For each additional processing operation, the controller shall previously inform the data subject and seek explicit consent to re-use the data. Related to the purpose limitation also, the amount of gathered data has to be strictly limited to what is necessary to fulfill the pursued specific purpose, meaning that some data can be gathered for specific reasons and so to hinder excessively detailed and unnecessary amounts of personal data. Once the data has been gathered, the controller cannot store them indefinitely. To limit such cases, the GDPR envisioned equipping stored data with a sort of expiration clause; in other words, once the personal data are no longer needed to fulfill a certain processing operation, they shall be deleted. Data at rest and also on the move are inevitably exposed to cyber-risks and hacking by cyber-criminals; in order to preserve their integrity and confidentiality, as so not to harm in any way the data subject, the controller shall adopt utmost care and appropriate technical and organizational measures to prevent risk scenarios that could lead – i.e., to a data breach. During these activities and the data lifecycle, both controller and processor bear the full liability and so should be able to demonstrate at any given moment that overall compliance of their internal operations regarding personal data; thus, they are accountable for their action.

2.3 Main Rights of the Data Subject

Since part of the scope of the GDPR is to provide data subjects with a reasonable and exercisable control over their personal data, the European legislator has envisioned a series of rights and instruments that form the *toolbox* to be used when the data subject autonomously and freely decides to exercise them.

2.3.1 Information

Art.12 explicitly states that the controller, upon request of the data subject, shall provide any information pertaining to the data subject without unnecessarily delaying the completion of said request, and if so, the reason shall be communicated to the data subject. Both the form and content of the communication have to meet certain requirements further set out by law; upon deliverance of the requested information, the processor has to present the latter – as stated in para. 1 - in "a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child, "if deemed appropriate, even including the use of standardized icons or other visual supports. Said communication shall happen only upon identification of the data subject so as not to divulge personal information to third parties and free of charge. Art.13 further sets a series of content requirements as to what the communication received by the data subject should include. Among the many, the controller should include the contact information of both processor and controller – if applicable, the purpose of the processing as to state why personal data are gathered and under which legal basis. The time extent for which the data will be stored must be included along with the usage of Automated Decision-Making instruments (ADM). Aside from the general information about the processing parties and the undertaken activities, the communication to the data subject must include an explicit statement that informs the data subject about the existence of other rights, such as the right to lodge a complaint with a supervisory authority, to withdraw consent, demand the access, rectification, or deletion of one's personal data as well as the right to restrict further processing and transfer data (data portability).

2.3.2 Access

Through the right of access, the data subject is able to request confirmation from a controller that his or her personal data are being processed by the controller. Where this should be the case the data subject can demand to access his data and receive further information about the purpose of the processing, the categories of personal data involved, the recipients to whom the data have or will be disclosed as well as the storage time and its extent Furthermore, the controller will have to include, as already seen for the right to information, the available tools and rights for the data subject as well as the ability to request a copy of the personal data currently undergoing processing. In this way the data subject is able to see what is being done with his or her data and which ones are currently being used.

2.3.3 Rectification

(Big-) Data are considered to be messy and inexact, leading to a true Copernican revolution of data analysis. Cukier and Schönberger (2014) have highlighted both benefits of massive and messy datasets in the making of predictions and data analysis that embraces chaos as a resource rather than a fault to be eradicated. Although this might be true and tolerable under certain aspects and conditions of application, messy personal data – thus inexact if not misleading ones – can have seriously detrimental effects on the data subject. To avoid any form of significant harm for the natural person that is the data subject the GDPR grants the ability to demand the rectification (update) of potentially wrong personal data.

2.3.4 Deletion

The right to deletion, also known as the “right to be forgotten,” provides the data subject the ability to request the complete deletion of his or her personal data. The deletion request is not absolute, meaning that a data subject, maintaining the complete ability to advance said request may see his data deleted if one of the following conditions is met. For the data to be deleted the latter must no longer be necessary for the purposes for which they had been gathered in the first place, the legal basis for the processing no longer exists or the data subject has withdrawn consent, the data have been processed in an unlawful manner or to meet compliance with a union or member state law the controller is subject to. The data deletion is further made possible if the data have been collected to offer information society-related services[5] . As already said, the deletion of data is not absolute and is inapplicable where the deletion of said data affects freedom of expression and information, data are required to comply to union or member state laws or the fulfillment of tasks carried out in the public interest by authorities, for reasons of public health, for the establishment, exercise or defense of legal claims, as well as for archiving, research, statistical and historical purposes.

2.3.5 Restriction of processing

The restriction of processing can be obtained in cases when the accuracy of data is contested so to enable the controller to verify and act accordingly, when the processing is unlawful, and the data subject objects the erasure of data and opts to restrict their use or when the data subjects challenges the legitimate interest established by the controller as it overrides the interests of the data subject himself. Furthermore, the restriction of processing is applied when the controller no longer needs the acquired data, but the data subject needs the data not to be erased to allow their use in legal proceedings for the establishment, defense, and exercise of legal claims.

[5] art.1 (1) (b) directive 2015/1535: ‘service’ means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present; (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.

2.3.6 Right to object

The data subject can object, at any time, to the processing of his or her personal data. To further continue processing operations the controller will need to prove that the legitimate interest upon which the processing is based overrides the interests' rights and freedoms of the data subject.

2.3.7 Data Portability

The data subject has the right to request data in possession of a controller to be directly transferred to a second controller without any hindrance from the controller who received it in the first place. In addition, the data subject can request to receive their personal data to act directly as an intermediary between the first and the second controller.

Despite the presented instruments the data subject can enact against a controller, it becomes evident that the user's ability to exercise complete control over their personal data appears limited and sometimes hardly enforceable without adequate knowledge of data protection laws. Overall, the amount of control the data subject can enforce is still a concession since the process requires a request to be made, potentially without any available proof that – for example, the data have been truly and diligently deleted, in some way still relying on trust to confirm that the requesting parties demand has been met. Therefore, the central entity that is the controller still maintains an exceedingly high degree of control and, in a certain way, fails to fill the intrinsic power asymmetry digital services feature. It has been said that blockchain has a confirmed disruptive potential. Its core functioning, which deposes trust-based interactions in favor of trustless ones, might come in useful in both simplifying the enforcement of data subject rights in an increasingly complex and datafied6 environment while allowing users to exercise a greater degree of control over their data finally; that sooner rather than later might become even more valuable than they are today. Starting this small yet powerful change in mindset is the start of a new understanding of the constructive and non-opposing relationship between technology and legal compliance.

2.4 How is blockchain affecting the governance of data protection.

Until now, the GDPR has been the sole regulatory measure ensuring that private and public parties that necessitate processing personal data in their business activities lawfully use these while ensuring that the data subjects (users) are equipped with a series of rights to protect themselves from illicit data exploitations. Accountability requires identifying one or more entities that will bear responsibility for a certain activity and events that may happen. In this particular case, the GDPR has identified two main roles responsible for the processing activity and that are directly and indirectly responsible for it.

2.5 Privacy roles: Controller & Processor

Taking into consideration the definitions provided by the GDPR in Art. 24.

> 'controller' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;[6]
>
> […] The controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.[7]

The controller is, therefore, the owner of the processing activity and, as such, is considered to be both liable and responsible for any incidents or illicit behaviors related to the processing activity. The controller might directly undertake to process or, optionally, delegate the operational part of processing to a second actor, the processor. As per definition, the processor is any natural or legal person, public agency, or other body which processes personal data on behalf of a controller.

> The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.[8]

[6] Regulation UE 679/16 Art. 4 (7)

[7] Regulation UE 679/16 Art. 24 (1)

[8] Regulation UE 679/16 Art. 28 (2)

The processor is further prevented from acting outside of the received instructions by the controller unless required to do so by Union or Member State law. These two actors envisioned by the GDPR are therefore framed within the context of organizations or any other centralized entity that deals with data to sustain their business model partially or totally. Blockchain has been presented as a radically opposed tendency to the current centralization tendency the global platform economy has been built upon, opposing the former through an increasingly decentralizing trend. This increased decentralization poses a considerable concern for supervisory authorities, enterprises, and data subjects when adapting traditional privacy roles and their responsibilities in the blockchain era.

Concerning the possibly momentary necessity to adapt data protection and privacy measures as the legal and technological landscape are evolving appears to be a rather challenging task when considering that the context and systems for which they were originally designed are evolving, if not giving way to new ones.

> The GDPR, and more broadly classical data protection principles, were designed in a world in which data management is centralised within specific entities. In this respect, the decentralised data governance model used by blockchain technology and the multitude of actors involved in the processing of data lead to a more complex definition of their role. (CNIL, 2018)

It has been said that within a blockchain, both permissionless and permissioned, the nodes contribute to the tout-a court governance and functioning of the blockchain being so effectively considerable as shared owners of the system itself. Since blockchain participants are also able to democratically define the purposes (objectives pursued by the processing) and the means (data format, use of blockchain technology, etc.) of the processing (*ivi*), they technically – under the current definition – qualify as (shared) controllers. The CNIL (*ibidem*) further advises against joint controllership, as defined under Art. 26 of the GDPR, since this would require the parties to assign respective responsibilities among them. Considering the size, a DLT architecture can reach, the CNIL (*ibidem*) suggests identifying a controller beforehand to overcome unnecessary complexity. On the other hand, miners are not considered controllers since they merely share their hardware, and so elaboration power in POW Blockchains to validate a transaction without defining purposes or means of processing, therefore acting as mere disinterested (techno-) logical facilitators; within the meaning of the GDPR they would, in some way be considered as processors if personal data are being processed on the blockchain.

2.6 Going Beyond– The future of Data Protection

As the technology and the relevant regulations, so do rights and duties and how they shall be enforced. Blockchain has certainly produced a significant shift shaking the way data protection will be conceived from now on, starting from the core principles the GDPR is built; in order to understand how the future will look like, the relationship between technology and law should be taken in consideration starting from how they mutually empower, depower, or shift form.

Looking first at how blockchain functions, some mechanisms and features – in other words, affordances – are more than they are on the surface. The complete transparency and inalterability of stored information as well as decentralization and user empowerment achieved through consensus mechanisms and cryptography, is part of the true essence of the technology deeply rooted in its protocol.

The GDPR envisioned a series of principles to protect personal data starting from how data shall be processed and stored. Once a block is created and processed, it is inserted into the sequence of other blocks making it exceedingly difficult to be deleted or altered in any other way. Under the pure technological light, this is a distinctive and functional feature that presents a major concern when personal data starts being involved and stored on the blockchain.

The principle of storage limitation appears, under these circumstances, to be incompatible and inapplicable in blockchain environments since each block – of potential Personal Data – is necessary for the continuity and functioning of the entire system: just like playing cards can be stacked one on top of the other to create a castle; none of them can be arbitrarily deleted but only added on top of all the others, otherwise the entire castle would collapse. The time-wise inability to dispose of data once they served their scope has a further spillover when considering that the accuracy of personal data might be endangered.

Human error might lead to wrongly entering data without having any possibility to alter them, whereby the right to rectification and accuracy of data is explicitly mentioned in the GDPR to prevent any detrimental harm to the data subject. In this case, additional technical and governance measures shall be established to adapt the technology to the law. In contrast, in the previous case, the law must adapt to the technological requirements.

Besides the storage limitation and data accuracy, other principles such as integrity and confidentiality find a new degree of enforceability under what technology allows. Although, as will be further discussed, cryptography does not constitute the best possible solution to safeguard the integrity and confidentiality of data; even more, if personal data are involved, the fact that cryptography integrated by design into a system leaves only room to again, add safeguards rather than removing them. There is some obvious and necessary work to do to fill some of the shortcomings on both sides to thrive in the future. However, many potential benefits appear to achieve a new status enforced by technology. What was previously a regulatory requirement, possibly formalized by law or international standards and assessed by regular audit controls, can be backed up not only from a legal standpoint but also from a technological one. At this conceptual intersection, code as a law (Lessig, 1999) and law as a code meet and mutually influence themselves to expand, innovate and shape comprehensive governance to protect personal data and data subjects beyond the traditional boundaries and conceptions of personal data protection as will be further explained.

2.7 Data subject and blockchain: a positional reversal for empowerment

Although the regulatory landscape, as well as the technological one, both need to cooperate and adapt according to their mutual needs, if the effort to reconcile “what law wants and what technology is” might bring significant benefits for society, including the creation of a data self-governance system. In the previous chapter a comparison has been presented between the before and after blockchain adoption where, among the many differences, an interesting phenomenon could be observed regarding the user’s position in the exercise of powers and rights against intermediary entities. Regulations like the GDPR clearly find their purpose when considering the necessity to provide data subjects with the necessary toolbox to create a line of defense against any potential exploitation of their data since little to no control can directly be exercised over them.

Blockchain ecosystems radically reshape the assumption that users lack any decisional power simply by including them into the governance system through the consensus mechanisms as well as substantial freedom to store anything inside a given block but also with new powers and capabilities including personal data self-governance definable as the capacity of data subjects to copy, change, share and move their data (Fink, 2018, p. 34); as they have become our society’s new [digital] gold conceded by all, convened by many and effectively controlled by few.

Chapter Three: New technologies, needs and regulatory requirements.

3.1 Compliance

While exploring the contents, current requirements and obligations set out by the GDPR, the *privacy by design* principle is certainly the most important when it comes to the regulation of new technologies and their sustainable processing of personal data; especially when considering the disruptive potential of blockchain technology and the risks a failed regulation attempt might pose for personal data. The need for a mutually initiative-taking attitude towards the problem might even decide the future of blockchain's ability to enter the mass market, finding new applications and bringing potential new benefits, products and services to societies.

Since the global blockchain market is thriving and so are concrete blockchain applications the CNIL (2018) has gathered a series of recommendations to be observed when deciding to implement such technology in a digital product or service. In line with the risk-based approach, the responsible entity for the implementation shall, first, conduct an extensive evaluation aimed at assessing – whether – the use of said technology could truly be considered beneficial without exposing the entity or the users (including their data) to unnecessary risks minimizable by preferring alternative technologies.

Hypothesizing that, a given blockchain-enabled product or service ought to be considered as safe and appropriate it is still necessary to consider the appropriate technical, technological and governance measure that allow for an expansion and improvement of data rights rather than their compression. For these specific reasons, the mutual innovation and cross contamination between law and technology is crucial to understand how the conception around data protection, digital rights and privacy will evolve in a society that already is, and further will become, increasingly connected.

3.2 Technological Measures

Among the best practices Supervisory Authorities have issued concerning Blockchain technology applications, the preference for permissioned blockchain protocols stands out since, as previously presented, they feature a greater degree of control over the nodes that translates into a more stable, secure, and accountable eco-system. Conversely, public permissioned blockchains are rather discouraged as their vulnerabilities exceed their resiliency capabilities, unnecessarily exposing the participants and the content of each block to non-neglectable cyber risks.

3.2.1 Data Format

“By Code” blockchains leverage cryptography as the cornerstone of every protocol; in a certain sense, cryptography can exist without blockchain, but blockchain cannot exist without it. Users have become acquainted with the idea of cryptography being the top-tier solution to secure their digital assets, including information and data. Despite SHA-256 being one of the most currently advanced and widespread hashing algorithms, contextually to the evolution of hacking tools and practices, it appears to constitute a rather basic, although a fundamental, layer of security and confidentiality.

In compliance with the purpose and storage limitation the CNIL (2018) advises to better consider the content of each block. As already seen blockchains are additive technologies meaning that each new entry is as necessary as the previous one to keep the ecosystem together. This regards the identifiers each participant is equipped with, more specifically each block contains a public[9] key (identifier) formed by an alphanumeric string. This apparently random string serves therefore multiple purposes, among which the structural one stands out. The second component is the payload, or additional data, that a participant wants to store. This additional payload is of crucial importance considering that it may potentially contain anything, but more importantly personal data.

The Privacy by Design clause, found in Art.25 of the GDPR

> requires the data controller to choose the format with the least impact on individuals’ rights and freedoms. […] Personal data should be [therefore] registered on the blockchain preferably in the form of a commitment […] [Avoiding so to store the payload in clear text]. (CNIL, 2018, *pp.* 6)

3.2.2 Commitment Schemes

The CNIL, in particular, advocates for the use and implementation of additional layers of encryption as the baseline that SHA-256 by design is not considered sufficiently capable of filling the gap between technology and GDPR compliance when personal data are involved: since, as already assessed, blockchain technology significantly alters the conception and implementation of GDPR rights through its simple existence (see 2.6 for a preliminary assessment). Commitment statements are cryptographic protocols that allow two parties (A and B) without requiring the statement to be communicated or allowing it to reveal at a later stage. They find a wide array of applications but can generally be used in cases where the two interacting parties do not necessarily trust each other.

Hence, Commitment schemes mimic the purpose and functioning of an armored safe. The utility of commitment schemes can be sought in the different features of this cryptographic protocol. Commitment schemes are by-design:

[9] The Public key can be freely shared and publicly exhibited contrary to the private one which has to be securely guarded by the owner.

a. Binding: The commitment must be binding, in the sense that it is not possible to change the committed value without the commitment being detected or revealed. This is achieved by making the commitment function one-way, such that it is computationally infeasible to find another value that hashes to the same commitment since they are also collision resistant.

b. Hiding: The commitment does not reveal any information about the committed value. This is achieved by adding a randomizing factor to the value being committed to, which makes it impossible to determine the original value from the commitment alone.

c. Non-malleability: The commitment must be non-malleable, meaning that it cannot be modified without being detected. This is achieved by using a commitment function that is resistant to tampering. Otherwise, the ability to arbitrarily modify the committed value would defy the purpose and logic of the whole protocol.

d. Computationally efficient: The commitment scheme must be computationally efficient, meaning that the required energy input and computational power should be reasonably balanced between being secure and affordable as the higher the security the more expensive the computation and creation of the commitment gets.

e. Universally composable: The commitment scheme should be universally composable, meaning that it can be used in combination with other cryptographic protocols without compromising its security.

Having explained the general features of cryptographic commitment protocols it could be useful to provide an overview of the different steps that comprise the creation and operation of the protocol at stake.

1. Commitment: The committee, the party who intends to commit to a value, chooses the value they want to commit to generating a commitment (C) for that value. The commitment can be described as the combination of the input with addition of a randomized numeric value that can be described as follows: $C = (input + random\ number\ sequence)$[10]. The commitment is generated in a way that makes it computationally unfeasible -or rather unsustainable- to determine the original value from the commitment alone as this operation would require a considerable deployment of resources, mainly computational power and energy, as well as time.
2. Concealment: The commitment is then shared with the other party as-is without revealing any information about the committed value, the random number, or the key that was used to encrypt it.
3. Opening: The party who made the commitment (sender) reveals the original value and the randomizing factor used to generate the commitment. This step proves that the original value was the one committed to in step 1.

Commitment schemes are particularly used in Zero Knowledge Proof (ZKP) which is a cryptographic concept that allows one party (the prover) to prove to another party (the verifier) that a certain (commitment) statement is true without revealing any additional information beyond the fact that the statement is true. Thus, it enables private transactions on a blockchain, where the details of the transaction are hidden from everyone except the parties involved, with the capability to keep certain information confidential. ZKP is particularly useful in personal [digital] identity management as personal data and potentially sensitive information find a new layer of safeguard. Albeit the importance of said encryption protocols is necessary, it shall be underlined that their application remains a preferable outcome rather than an obligation, meaning that a case-by-case assessment has to be conducted to understand if their presence is effectively required. The criticality around the concept of personal digital identity will be explained in greater detail in the next chapter, also presenting how this new form and extension of offline identities find new ground for social and legal concerns in the online afterlife.

[10] Similar mechanisms are used to protect passwords and sensitive information from being easily decrypted. In cryptography, salting refers to the process of adding random data, called a salt, to the input of a hash function to generate a unique output. The salt is usually a randomly generated string of characters added to the plain text before it is hashed. The result of the hash function is then stored along with the salt. The purpose of salting is to make it more difficult for attackers to crack passwords or other sensitive information. Without salting, an attacker could use a pre-computed hash table, a rainbow table, to rapidly decrypt. However, by adding a unique salt to each plaintext input, the resulting hash is also unique, making it more difficult for an attacker to use precomputed tables to crack the password.

Chapter Four: Existing in Cyberspace

4.1 Web 2.0, society, digital identity and legacy

Information society services – especially social media- have radically reshaped individual and collective communication, economic and general interaction practices empowering the individual's mass self-communication (Castells, 2007). With the rise of digital platforms and the ever-increasing importance of social network sites, among the many, personal data and their crucial role in fueling platform business models has led to an increasingly strong demand for regulations, data security, protection, and compliance. Together with the ability to freely – although to a certain degree – self-communicate (ibidem), re-present, and shape one's identity through the creation of many different profiles have further contributed to reconsidering the very concept of personal identity *in toto*.

> In a rather obsolete conception, personal identity was understood as the whole of the official personal data resulting in public records, and important for the public purpose of making the citizen identifiable by the public administration: name, pseudonym, date of birth, address, status, and so on. (Pino, 2000, *pp*. 1)

It shall be highlighted that the concept of personal identity, as defined in case law, relies heavily on the role of the public authority and its sources –public records- in which personal data are stored to make citizens (individuals) recognizable and identifiable through the use of a series of identifiers or "Piece[s] of information that acts as a pointer to a particular identity or identities. Common identifiers include among the many: Name, Surname, Social security number/tax ID number, Mobile number, Date and place of birth."[11]

> Identity [at least traditionally speaking] is not something that individuals are able to create by themselves, at least under the legal and administrative understanding, but something that is "attached to a human being, separate from him or her [thus not following under his or her control]" (Romanov et.al, 2017).

For the sake of completion, it should be mentioned that public administrations have been experimenting with establishing digital identities in the last years, effectively allowing users to log in and register to selected and eligible services with the same set of credentials used on national IDs. Although this could signal the pretext for mass adoption of this kind of identification and registration practices, a centralized identification system would lead to the entire World Wide Web being subjected to one or few selected identification agencies, creating a rather dystopian version of the Internet society we know.

[11] https://ethereum.org/en/decentralized-identity/

In the latter case, no public body or authority can guarantee that the information provided by the user is accurate, dependable, and moreover make him or her unequivocally identifiable – the result is what people started calling an avatar. The word *avatar* comes from Sanskrit अवतार *avātara* which means “descent or incarnation” and is used to indicate the incarnations of the God “Vishu” who, according to the Hindu tradition, can take ten different forms. Avatar gradually started to indicate the user's tendency to “incarnate” themselves in different forms while subscribing to different online games or sites.

If on the plane of reality, a person is identified and made identifiable unequivocally, online he or she can project and create infinite different forms just by subscribing with new credentials. An online profile usually contains “a picture and name, possibly an [e-mail] address and birth date […] (Romanov, et al., pp 363, 2017) along with a username, or handle, that uniquely identifies the user within a certain platform system, some if not all of the previously mention information qualify under the GDPR as Personal Identifiable Information. These profiles are not empty boxes as will be further discussed but, in fact, can contain many other heterogenous elements (including digital access credentials, email addresses, usernames, social media accounts, avatars and multimedia contents) that can characterize a given person beyond the traditional meaning of identity.

4.2 On-life and digital legacy

Online interactions, from the simplest ones to more complex tasks leave a digital trace of which the users are sometimes aware of, whilst other times remaining undetected.

> Many users have been connected for many years and have accumulated a large amount of data [and UGC]; thus, a real digital life has come into being, linked to a digital identity [...] that has been enriched day by day [...] (Ziccardi, 2017, *pp.*71,)

All that messages, photos, and other UGC (User Generated Content) created by a given user are not only *“bits and pixels”* but are elevated to memories, assets, or even traces of a person’s life that have been uploaded and shared online; in other words, they have and will have a precise meaning these become a new form of *digital asset* and *legacy.*

A broadly accepted definition of what has to be understood as digital legacy since clear definition still does not exist. As an example, a digital legacy can be constituted by two large categories of physical and immaterial goods. Ziccardi (2018) presents a further categorization level offered by Legacy locker a startup in the digital afterlife industry (DAI) (Floridi, 2017). A larger distinction is first presented between *physical legacy* (encompassing traditional inheritable assets) and *digital legacy*, which is strictly related to the digital existence of a given individual. In the first, Smart devices, Hard Drives, USB or similar can be included. The second category embraces online profiles, e-mails, Direct messages, UGC content, cryptocurrencies, and NFTs. Paying close attention to this second category, it is clear that – a considerable part close to the entirety of the user’s digital trace (footprint) - can be considered an immaterial digital legacy.

Within the larger category of digital legacy, a further distinction can be made between financial and emotional assets. Within the sub-category of digital financial assets, Cryptocurrencies, and NFT might find a better collocation with possibly particularly valuable in-game assets. Leaving in the emotional sub-category space for social media profiles, UGCs, multimedia, and other assets qualifiable as memories.

Assets			
Online			**Offline**
Material PC, Smartphone, USB, HDD	**Immaterial** Social media profiles, UGC, NFTs, Crypto		Car, House, etc..
	Emotional Social media UGC (digital memories)	**Financial** NFT Crypto	

As the proposed categorization sheds some light on the complexity of digital assets, it should be considered that a clear-cut separation is not always possible. Digital assets are liquid and dynamic entities that gain or lose value, potentially emotional as well as financial – based on a multitude of factors that cannot always be accounted for; a further layer of complexity is then added when considering how different digital assets are regulated by law in case where they become part of a larger inheritance. Hence, for the sake of clarifying and defining the boundaries of this research attempt, particular attention will solely be dedicated to those digital assets that might or might not contain strictly personal information with no financial value.

Now that both digital identity and legacy concepts have been explained, some additional observations can be made. As already assessed, a user's digital identity is a self-constructed – rather than imposed – a system that, through social media, allows users to "manage both their social network [social relations] [...] and their [digital] social identity" (Riva, 2016, *pp*.15). Digital social identity is, in a certain sense, the means through which a user presents himself to a larger digital network; and does so by continuously constructing a digital identity.

This generative process happens not only upon registration but also through the constant creation and interaction with User Generated Contents (UGCs), which allows us to logically conclude that a digital identity is essentially formed by its digital legacy in the form of emotional, financial assets, personal data and many more; In other words, it is.

> […] an informational structure; a narrative constituted by everything that defines it: memories, biometrical information, search history, social data, and so on. Thus, people do not merely own their information, but are constituted by it, and exist through it. (Floridi, 2017, *pp.*649)

$$Digital\ Identity = Digital\ Assets = Digital\ Legacy$$

As the growing importance of digital self-representation and identification, datafication has led to a tech-driven expansion of individual, collective, and social interaction; this has inevitably further spillovers on how physiological and digital existence are conceptualized.

The "end of life' in the physiological and biological sense of the term, has a beginning – birth – a course – growing and thriving – and eventually an end – death. A Digital identity's lifecycle follows a similar path as the biological and offline counterpart amid some differences that can be observed, especially regarding the end of life. Once a new digital identity is "born" upon the creation of a social media profile – an avatar- it grows and thrives as its owner uses it more or less regularly. For one reason or another, at one point, a given person could decide to delete the account, and so a part of his or her digital identity "dies." Digital death, in this sense, is the last step of the process of one's account deletion, a someone voluntarily undergoes. Under different circumstances, a profile can metaphorically "die" as the consequence of a Terms of Service (ToS) violation which is met with the cancellation or suspension of the incriminated profile; this can also result from perpetrated inactivity.

While other times, inactivity can be the result of many different scenarios such as loss of interest towards the service, loss of credentials or more tragically the death of that particular user; this would be the only case where the digital identity of an individual outlives biological existence. Meaning that, after a person's death his profiles and so his online presence and contents are all – potentially - still online as if the recently deceased users were still alive and (in)active[12].

The increased concern for "dead profiles' has been around for quite some time, which led the more popular platforms such as Facebook (now META) to seek a solution to avoid their platform spaces resembling e-graveyards populated by digital zombies as they do not only pose a concrete threat from an information security and data protection perspective but also threatens the deceased dignity and the heirs' ability to regain control over potentially relevant, sensitive as well as valuable digital assets.

[12] Twitter, as per new policy, has a maximum inactivity period of 30 days after which the account is permanently disabled. https://help.twitter.com/en/rules-and-policies/inactive-twitter-accounts#:~:text=What%20is%20Twitter's%20inactive%20account,removed%20due%20to%20prolonged%20inactivity.

4.3 Social media and the afterlife

Social media and the web have radically reshaped both collective and individual communication and self-presentation practices. Daily, people share parts or their entire routines, experiences, and memories through photographs, videos, and other multimedia content, uploading them on their profiles to be shared and exhibited: while simultaneously, if not unconsciously, opening up their private sphere. Social media, according to boyd (2010), identified four cardinal elements that constitute the essential scaffolding of a social media platform:

1. **Persistence**: social media encourage and thrive on their ability to store multimedia contents for very long periods of time in order to allow for asynchronous interactions to activate around them; in other words, they exhibit a tendency to remember by default. Great attention will be put on this peculiar affordance as it relates to the individual ability to voluntary leave a trace, as well as enabling the ability to autonomously create a personal narration.
2. **Scalability**: social media allow users to share their contents with very large audiences, hence exhibiting a tendency for content virality. All these interactions are therefore public, visible to anyone worldwide and remain so by default, unless the users specify the contents to become private (Bentivegna, Boccia Artieri, 2019)
3. **Replicability**: Contents can be indefinitely replicated, duplicated, and diffused
4. **Searchability**: As a content is shared, its persistence and wide visibility makes it possible to be sought over time, unless it is deleted or rendered private.

[…] [Social media are] space[s] where users can narrativise their lives as well as an archive of messages between users,' and thus embodies 'evidence of the production of personal identity through social interaction that takes into account the multiple pasts and presents that the user has occupied/is occupying' (Garde-Hansen, pp.147 ,2009).

The archival functions (**Persistence** and **Searchability**) become crucial if tied to the tendency above of digital identities to outlive individual biological existence.

> [As] Online identities survive the deaths of those they represent, leaving friends and families to struggle with the appropriate ways to incorporate these [digital] identities into the practices of grief and mourning (Brubaker, *et.al*, 2013, *pp.*152)

Overall, this poses an inevitable concern on the side of the Platform providers to deal with the increasingly emergent necessity to reconcile the right to mourn online with the obligation to safeguard digital identities in the afterlife. But what can be feasibly done to mitigate risks and allow these new forms of digital bereavement to develop? What happens concretely to the deceased digital identity? What else can be done?

4.3.1 Business as Usual:

Among the many possible courses of action to manage someone's online presence after death, the most straightforward and possibly less secure option is to leave the profile as it is. Theoretically and practically, this means that the profile appears inactive but can still be accessed with regular access credentials or maliciously hacked; this further exposes the content and potentially sensitive information about that person to potential malicious use. Inactivity, or the abandonment of profiles, is not sometimes a choice but could result from the account's existence being unknown to immediate family members and friends.

Sometimes – such in the case of Google[13] – self-destruction function will delete all information, but not the profile itself, after no login history has been detected in more than 24 months; additionally, users can set a lower inactivity period from their account. Not every social media or internet-related service has an inactive account deletion policy meaning that accounts are simply abandoned without any safeguard besides the access credentials.

[13] Google recently introduced an Inactive Account Manager that enables the account owner to set up a customized inactivity period upon which the account will be deleted. https://support.google.com/accounts/answer/3036546?hl=en&sjid=1869111665463341259-EU

4.3.2 Facebook’s memorial account

Max Kelly, Head of Security at Facebook highlighted this particular issue in a post where, upon losing a friend and colleague of his, the question of what to do with his Facebook profile arose.

> Obviously, we wanted to be able to model people's relationships on Facebook, but how do you deal with an interaction with someone who is no longer able to log on? When someone leaves us, they don't leave our memories or our social network.
>
> To reflect that reality, we created the idea of "memorialized" profiles as a place where people can save and share their memories of those who've passed. […] When an account is memorialized, we also set privacy so that only confirmed friends can see the profile or locate it in search. We try to protect the deceased's privacy by removing sensitive information such as contact information and status updates. Memorializing an account also prevents anyone from logging into it in the future, while still enabling friends and family to leave posts on the profile Wall in remembrance […] so their memory can properly live on among their friends on Facebook. (Kelly, 2009)

To transform a profile into a memorial account a request has to be directly submitted to Facebook, within the request module Facebook will ask for the profile URL, the date of death as well as an official document so to avoid any potential errors.[14]

> This ‘immortalisation’ element of memorialised profiles raises the curious prospect that constructed identities [digital identities] can survive, at least in some form, after the biological death of that identity's ‘bearer.’ As we saw above, the identity constructed in these anchored online environments is an extension and expression of the socially constructed, largely intersubjective dimensions of our everyday practical and corporeal identities, of ‘who we are in real life.’ What the Facebook profiles of the dead seem to suggest is that our social identities are not necessarily coextensive with the biological life of the individual human organism with which they are associated, and thus it is not the memory of the dead person that is being honoured and sustained through this form of memorialisation, but some dimension or extension of the dead person themselves. (Stokes, 2011, *pp.* 367)

[14] https://www.facebook.com/help/contact/234739086860192

4.3.3 Legacy Contact

Legacy contacts are part of Facebook's digital death policy and are strictly related to the memorialization function of the account. Legacy contacts can be nominated *in life* directly by the account holder. Facebook clarifies that Legacy contacts cannot[15]:

1. Log into the memorialized account.
2. Remove or edit past posts.
3. Read messages.

Hence, the appointed person does not inherit the account they have been nominated to "administer," they rather function as intermediaries between the deceased and it is will and the platform. What legacy contacts can therefore do is[16]:

1. Manage a memorialized account.
2. Write a pinned post for the memorialized profile.
3. Respond to new friend requests.
4. Update the profile picture and cover photo of the memorialized account.

4.3.4 Deletion

Beside the possibility to set up a "digital shrine" on social media upon death a user might have a different wish.

> Such [digital] life, like real life, may be connoted by secrets, and may be characterized by information that an individual intends to keep confidential after death. This means that the death of a user who has constituted, over time, a digital legacy concerning him or her may entail as a priority, and a real and unfailing need. the request that certain content-photographs, videos, e-mails or other documents-be kept inaccessible by third parties or that, even destroyed; [metaphorically dragging everything into the grave]. (Ziccardi, 2017, *pp*.71)

[15] https://www.facebook.com/help/991335594313139

[16] *Supra note* 14

To comply with this “last wish,” beyond the right to be forgotten and data erasure in life, family members can request a dead account to be taken down by providing adequate information of *proof of death* (PoD)[17]which again requires the upload of the death certificate. In absence of said certification Facebook mentions a list of other possible documents that are able to demonstrate proof of authority such as:

1. Power of attorney.
2. Birth certificate (in cases where the deceased is a minor).
3. Last will and testament.
4. Estate letter.
5. Submit one document to provide proof that your loved one has passed away:
6. Obituary.
7. Memorial card.

In other cases, the profile owner can ex-*ante* decide the fate of his accounts by filing a sort of Do Not Resuscitate (DNR)[18] that will require the nominated heir to necessarily delete the account with no exceptions.

> While some people might find comfort in the idea of living on digitally after they die, […] holes in data protection laws make it possible to virtually resurrect someone without their permission. […] the lack of regulation [or better said the deep asymmetrical regulation that exists] on the issue leaves the door open for others with access to the data of the deceased. (Bacchi, 2020)[19]

Deletion can also result as a consequence of the platform provider enforcing inactivity policies that lead to the complete loss of the account (and the content) if no activity is detected for a certain period of time, in the case of twitter as the most recent available policy states “[…] to keep your account active, be sure to log in at least every 30 days. Accounts may be permanently removed due to prolonged inactivity.” (Twitter, 2023)

[17] https://www.facebook.com/help/1111566045566400

[18] DNR Do Not Resuscitate is a medical order filed by a patient that enjoins healthcare providers to perform any resuscitation attempts (CPR)

[19] https://www.reuters.com/article/us-global-tech-privacy-trfn-idUSKBN21Z0NF Accessed: 07/04/2023.

As correctly highlighted by Bacchi (*ibidem*) this possibility concretely exists if considering how easy it is to fetch basic information such as name, surname, and profile picture if no safeguards are foreseen. But beyond the aspect and concern of personal dignity in the afterlife, the entire digital asset (identity) of the deceased user is inevitably still vulnerable. Going beyond the afore-presented privacy protecting technologies, the question of digital asset ownership and inheritance becomes crucial. Hypothisizing that a given profile is memorialized, all the information, contents and that that make up that digital identity of a particular user are still "owned" and controlled by the platform provider; or under the GDPR jargon the *controller*; thus, leaving immediate family members and heirs substantially unable to claim direct control or ownership of said contents beside what the platform allows to do.

Being still online and somewhat publicly available, although with significant limitations in terms of *Scalability* and *Searchability* (boyd, 2010), still leaves significant room for non-addressed cyberthreats such as data breaches as well as a possible exploitation of a particular delicate and sensitive moment for bereaving friends and family members. In the event of a similar cyber-attack, the memorialized account is still held "suspended' inside the servers and so potentially exposed to illicit misuse.

According to a more cynical line of thought social media platforms have an intrinsic interest towards "dead accounts' due to the legal uncertainty that currently affects personal data in the afterlife, this possibility will be further examined in the next chapter which also makes it harder for data subjects striving for a claim of control over one's own digital identity and assets. In order to empower users, an identity management system should give the individual ownership over their data [and identity], its use, distribution or non-distribution. "In effect, people must own the rights to their words, thoughts and data" (boyd, 2001, *pp*.71) effectively being able to turn them into THEIR inheritable digital legacy.

Chapter Five: Postmortem data protection: a European comparative approach

5.1 To protect, to own, to preserve

Nevertheless, the problem of digital death has been around for some time, as well as the individual one on misuse of private information, and is still heavily debated due to the numerous implications and potential negative spillovers it can lead to. Reconsidering boyd’s (2001) statement on data ownership it is clear that the latter might become a pre-requisite to allow to digitally inherit someone’s legacy on substantial rather than formal level. The concept of ownership inevitably enables the owner not only to possess but also to access, control and take decisions about a particular tangible or intangible good including the profile – so to say the box – and the therein contained such as digital media (UGC) and other potentially personal data or information.

In chapter two, while presenting and analyzing the characteristics of the European General Data Protection Regulation (GDPR) certainly constitutes one of the virtuous examples worldwide in terms of governing the lawful, fair and transparent processing of personal data. The substantial approach of the GDPR if applied to the particular case of postmortem personal data and online digital identities suffers a considerable halt. In spite featuring a considerable amount of protection and control over one’s personal data “in life,” recital 27 of the same regulation explicitly mentions how “*This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons*.”

Nonetheless, this could appear at first glance as a fault if not the origin of shortcomings that limit the extension of said rights, as well as the right to what could be called “digital self-preservation.” This is true on a certain footing but, continuing reading the recital, the European legislators envisioned an area of action for Member States to autonomously decide if and how to govern the data of the deceased. Deferring to Member State the ability to arbitrarily govern on such a complex yet important subject matter with considerable implications on individual dignity and right to self-determination, inevitably acts as a counterforce for the attempt of achieving a standardized, uniform and equal protection of data-related rights across the entire European Union.

The presented solutions to leave profiles untouched, memorialize them or even delete them all together has highlighted that platforms have been trying to self-govern and implement digital death policies in absence of substantial and harmonized legal guidance, as in the European case. In the latter case the absence of any regulatory guidance both at European and national level concretizes the worst possible scenario for data ownership which Malgieri (2018) refers to as *Data Freedom*.

As stated in Recital 27, once the data subject biological existence comes to an end, his data are substantially free from any regulation-imposed limitations on processing for example. This concretely enables platform providers to freely exploit data for any given purpose that, as already expressed can potentially harm the deceased dignity as well as upset the bereavement process of family members and friends.

> Firstly, the non-protection of data of deceased data subjects could lead to a moral harm to their grief and memory. The mere fact of receiving emails or communications related to the deceased relative/spouse/ascendant could be harmful for the intimate sphere of the bereaved.
> Secondly, personal data of deceased data subjects might be used to better “exploit” the grief vulnerability of the bereaved. If we consider the case of personalized advertisements, under this scenario personal data about the deceased could be freely used in order to perform more effective and pervasive marketing practices, e.g., when details of the deceased person and his/her kind of relationship with the bereaved are transposed or reflected in personalised advertisements (videos, images, etc.) [on which many social media platform business models rely upon].
> Thirdly, personal data of the deceased data subjects could be used to infer information about the living relatives. (*ivi*, 2018, *pp*.4) Effectively expanding the concern for information security for the dead and the living.

Beyond the evident concern for moral harm, individual dignity and right to be left alone while experiencing the death of a close person; it can be assessed how the need to better frame the concern for deceased online data and identities becomes a wider problem for a society whose existence and cultural practice have become truly hybrid.

5.2 Member States

As already expressed in paragraph 5.1, the GDPR does not feature any clear guidance on personal data in the afterlife, effectively excluding any possible enforcement of Data Subjects' rights from a purely regulatory perspective. As this might spark considerable concerns at first sight, the apparent regulatory void that originates in the digital afterlife can still be "flilled" by individual Member States. A comparative analysis becomes therefore necessary to better understand firstly, if the inevitable regulatory asymmetry that originates can be considered detrimental or not, secondly if the same asymmetry and "regulatory void" can allow the emergence and market entrance of services leveraging technologies to achieve postmortem privacy and data protection that could be gathered under the umbrella term of Afterlife Privacy Enhancing Technologies (APET).

5.2.1 Italy

As every European Member State, Italy has issued a national legislative decree that rules the protection of personal data. The legislative decree (d.lgs 10 agosto 2018, n. 101) has updated the previous decree (d.lgs 30 giugno 2003, n.196)[20] that received the provisions contained in directive 95/46/CE of October 24th, 1995, firstly introducing the protection of personal data. Among the contents of the legislative decree 196 of 2003 art.2-terdecies (2018 updated) contains a series of provisions regarding the Rights concerning deceased persons (*Diritti riguardanti le persone decedute*).

Data protection rights related to a deceased person, according to Italian law, “may be exercised by whom has an interest of his or her own, or is acting as his or her proxy, or for family reasons worthy of protection.”[21] Hence, certain individuals are given, the power to exercise the (data protection) rights due to the person concerned after his or her death. Since “everyone” is able to exercise said rights – potentially also in absence of a mandate – this would imply that the dignity and in a certain sese “privacy” of the deceased could be endangered. For this reason, paragraph 2 contains a series of restrictions and limitations. Restrictions in this case can be imposed by law or limited to information society related services, i.e., social media, the deceased owner can ex-ante express directly referring to the platform provider the will to prevent any post-mortem access to the profile.

[20] Codice in materia di protezione dei dati personali

[21] See d.lgs 30 giugno 2003, n.196, art.2-*terdecies*

A similar “posthumous right to restriction and access” has been presented and observed when analyzing the different policies that META (previously Facebook) applies when managing dead profiles (see 4.3.4): as in the previous case the legitimate owner has – while still in life- present written communication to the platform provider (the processor) stating his will to avoid any access to his or her profile after death. Such an enjoyment request cannot be general and shall be, according to para.3, specific, free and informed and can be limited to the exercise of certain rights. For instance, the deceased can specify his or her data to be transferred but not deleted or to be deleted once transferred. Nevertheless, “[…] the prohibition cannot have a detrimental effect on the exercise by third parties of their property rights arising from the death of the person concerned as well as their right to defend their interests in court.” From a purely privacy-related perspective the Italian legislator therefore grants access to the social media profiles of the *de cuius*[22] provided that certain conditions are being met.

The question remains open what is concretely being inherited – or passed along – from a purely legal perspective. Social media platforms, or any information society related service – requires entering a contract for the provision of a given service whose nature, scope, functioning, and requirements are contained in the Terms of Service (ToS) each user is required to fill out at the moment of registration; although the content of these agreements is usually overlooked -if not ignored- by the better part of the active user base. The service that is being delivered is usually a connective service – a technological facilitator – that is provided by the service provider (the platform owner) to a certain user base, enabling the creation of their digital identities. Adopting this contractual perspective answers the afore-posed question by stating that even before claiming ownership over a profile or a content after the owner’s death *(de cuius*). The heirs, according to the established doctrine and the principle of “[...] *transmissibility mortis causa* of the contractual positions held by the deceased at the time of the opening of the succession and, therefore, of the full continuation of the contractual relationship […] [are] called upon to assume the same rights and obligations” (Marino, 2018, pp.180). The “heirs succeed to all existing bargaining relationships, assuming the same rights and obligations that existed with the *de cuius*” (Corona, 2017). Having considered that the contractual positions of the *de cuius* can be inherited, enabling the exercise of the data protection rights, some exceptions may apply. While assessing the nature and content of Art.2- *terdecies* of the Italian privacy code, together with the internal policies activated by META, hence memorial accounts and legacy contacts, it became evident that the deceased can express a clear will to limit (or rather guide) the processing of his personal data and so determining the “fate” of his or her digital identity.

[22] In matters of inheritance and wills with the Latin expression "*de cuius*" the ellipsis of "*de cuius hereditate agitur*," that is, the person whose inheritance is involved). When it comes to the deceased, we refer to them briefly and concisely so that we can identify the deceased, their property will be inherited. Additionally, *de cuius* can talk be used to refer to a living person who is making plans for his or her succession and testament.

Imagining that the *de cuius* has expressed (in life) a clear will about the management of his or her account, a legacy contact has been nominated. According to Facebook's policies (see 4.3.3) the legacy contact has a bounded action capability that is enforced and established at both national level (Art.2- *terdecies*) and from a private contractual footing by the ToS and internal platform functions.

Consequently, despite having heirs the right and ability to inherit the contractual positions of the de cuius, implying that this is the first step to access the account and its contents (digital identity) in case the de cuius has designated a person (for instance a legacy contact) or expressed a clear will in life (m*andatum post exequndum*) the heirs' action capability can be affected as the result of the existing legal framework, case law as well as private platform self-governance mechanisms.

5.2.3 Germany

Among the considered Member States for the sake of this comparative analysis, the German case exhibits a countertendency in terms of postmortem data protection. The *Bundesdatenschutzgesetz*[23] *(BDSG)* does not extend its protection in the afterlife.[24] Far from concluding that Data Freedom (Malgieri, 2018), hence no access, control, and subsequent ownership of personal data and digital identities can happen. The German Federal Court of Justice (BGH) was called to settle a dispute between the parents of a 14-year-old girl that suffered a fatal accident under suspicious circumstances as she was hit by an incoming subway train.

> The parties dispute[d] [the] access to the user account of a so-called "social network"[25] operated by the defendant. The plaintiff claims to be granted access to the account of her deceased, minor daughter maintained with the defendant and "the communication content contained therein". Alongside her father, she is a member of the community of heirs. Both parents were the decedent's legal representatives during her lifetime. (III ZR 183/17, *pp*.2, *para*.2)

Said account had been opened under the supervision of the parents on January 4th, 2011 (para. 3). After the accident (December 9th, 2012) the mother of the deceased girl tried to access the Account of her daughter and discovered that the account had been converted into a memorial one. As already stated in 4.3.2 once a memorial account is activated it cannot be revered, thus also preventing any further access or status reversal. In the context of the case and the subsequent investigation gaining access to the social media profile was of crucial importance to rule out any suicidal tendencies; and was further necessary as "The personal communication content in her daughter's user account had been inherited by the joint heirs (para 5). Among the reasons underpinning the denial of access to the account Facebook, the defendant, cited the enforcement of personal data protection, telecommunication secrecy, as well as the conflict between said request and Facebook's Terms of Service (ToS).

[23] Federal Data Protection Act

[24] See. https://www.twobirds.com/en/capabilities/practices/privacy-and-data-protection/general-data-protection-regulation/gdpr-tracker/deceased-persons

[25] The court ommited the name of the SNS but from news articles it is possible to retrace the SNS to be Facebook. See: https://www.bbc.com/news/world-europe-44804599

The court opposed this reasoning by stating that "[…] the user agreement between Facebook and the deceased is a contract that passed to the heirs by operation of law (Gesley, 2018). In the event of the death of the account holder of a social network, the user contract is generally transferred to his or her heirs in accordance with § 1922 para. 1 of the German Civil Code (BGB). Access to the user account and the communication content contained therein is not precluded either by the decedent's post-mortem right of personality or by the secrecy of telecommunications or data protection law.[26] The court further claimed that no violation of the GDPR can be assessed since the latter, as explicitly stated in Recital 27, is not applicable to deceased persons (para. 64,67).

In the end the German court settled the dispute by requiring Facebook to provide access to the account mentioning that the content of the account (the deceased digital identity among the many) had to be treated as "strictly personal documents" such as personal diaries and letters and as such are part of the inheritance. The establishment of a conceptual similarity between analog and digital documents therefore allows heirs (i.e, parents) to inherit them under § 2047, para. 2 and § 2373, sentence 2 of the of the BGB (*para*.49). As previously discussed in the beginning on the chapter, access becomes a prerequisite to data ownership and inheritance of the content(s) of the "inherited profile" that might include "posted" pictures, direct messages as well as personal data or additional contents that may contain them (para. 69, Sentence 1).

Exploring the German context beyond the mere legal aspects some associations such as "*Verbrauchszentrale*"[27] that mentions a series of "unofficial" ways to make the inheritance and posthumous management of digital profiles easier. Under the voice "Digitaler Nachlass" (Digital Inheritance). The suggested approach is to fill out a list of every owned social media with respective login credentials; additionally providing a statement on what to do with each account and the therein contained information. A person shall then be nominated to fulfill the will of the *de cuius*[28].

[26] Beim Tod des Kontoinhabers eines sozialen Netzwerks geht der Nutzungsvertrag grundsätzlich nach § 1922 BGB auf dessen Erben über. Dem Zugang zu dem Benutzerkonto und den darin vorgehaltenen Kommunikationsinhalten stehen weder das postmortale Persönlichkeitsrecht des Erblassers noch das Fernmeldegeheimnis oder das Datenschutzrecht entgegen

[27] Verbrauchzentrale is a German Consumer protection association.

[28] For more details see. https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/digitale-vorsorge-digitaler-nachlass-was-passiert-mit-meinen-daten-12002

To further demonstrate the increasing concern for disruptive technologies in the digital environment and their governance the German Working Groups "Digitaler Neustart" has issued a report in (2017) especially focusing on data ownership, Digital legacy and inheritance as well as blockchain and crypto assets.[29] Particularly on digital inheritance the working group has stated that "there is no fundamental need for mandatory regulation in the area of digital estates. The testator has sufficient legal means at his or her disposal to also order differentiated regulations for the transfer (or deletion) of (or deletion) of data files (e-mails, etc.), both by means of regulations made during life and by corresponding regulations made upon death. ("Digitaler Neustart," 2017, *pp*.406)

[29] Digitaler Neustart, https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf (15/05/2017)

5.2.2 France

The French legal framework with the law number 78-17 of 1978 on *information technology, files and freedom*[30], refers in Art.85 (1) to the concrete possibility of the *de cuius* to express "[…] instructions for the storage, erasure and communication of his personal data after his death. These instructions may be general or specific. The general instructions concern all personal data relating to the data subject and may be recorded with a trusted digital third party certified by the CNIL" [31] Similarly, to the Italian case, the *de cuius* maintains the ability to express (in life) a mandate to administer his or her personal data. Factually Art.85 further states that the designated a person upon the data subject's death. In absence of said nomination the heirs will take over the execution of the *de cuius* mandate and communicate the exercise of said data protection rights to the controller in the name of the deceased; going as far as overriding any contractual clauses contained in the ToS as "Any contractual clause in the general conditions of use for the processing of personal data which restricts the powers attributed to the person by virtue of this Article will be regarded as unwritten."[32]

Paragraph 1 of the above presented law states the possibility of the *de cuius* to express a *mandatum post exequndum* for the administration of his or her personal data which concretely enabled the designated administrators and eventually heirs to exercise the data protection rights of the *de cuius*, unless otherwise stated by his or her own will.

Paragraph 2 of the same article (Art.85) further considers the hypothesis of the *de cuius* mandate stating that the heirs will maintain the faculty to exercise, after the legitimate owner's death, limited to the necessity of performing certain duties and procedures:

> 1. For the arrangement and settlement of the deceased's estate. To this end, the heirs may access the processing of personal data which concern him in order to identify and obtain information on the administration and division of the estate. They may also be entitled to access digital assets or data concerning family heirlooms, which are passed down to heirs.
>
> 2. When the controllers become aware of his death. To this end, the heirs may have the user accounts of the deceased closed, object to the continued processing of personal data concerning him or have the data updated. If the heirs so request, the controller must justify, at no cost to the requester, that he has carried out the operations required under the preceding paragraph. Disagreements between heirs over the exercise of rights provided for in II will be brought before the competent Regional Court.

[30] Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés. https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article85

[31] Supra note 25 and https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf

[32] Supra Note 26

The last part of point (1.) has a solid pertinence to the issue of digital identity, especially considering that multimedia contents form a non-neglectable part of a person's digital legacy. Since heirs are therefore entitled to gain access to the deceased digital assets it could be reasonable to argue that a person's digital repository contained within one or more social media profile(s) can be an inheritable intangible good with emotional value.

Coming to Art.85(3) "All providers of online communication services to the public will inform the user what will happen to the data concerning him on his death and will allow him to choose whether or not to share his data with a third party designated by him." According to the content just presented, the data subjects have the right to be informed about the fate of their data, and so personal digital identity, after their death. Users are further equipped with the ability not only to mandate but to designate a third-party service provider that shall receive said data directly by the data processor. According to this last regulatory element it is feasible to imagine the possibility to request the exercise of the right to data portability for the creation of an online digital memorial outside of traditional SNSs or other information society services that currently offer this kind of functions.

5.3 Meta-privacy

From this brief comparative analysis, it can be appreciated how deeply the online environment and the different legal codes are intertwined. Despite data protection not always being evenly applied in the afterlife of data subjects this legal *grey area* appears to be usually well covered, or coverable, through civil law or other legal sources. The equivalence, such as stated by the German court in 2018 (III ZR 183/17), between online and offline goods is what concretely enables digital assets and identities to become a legitimate inheritable asset.

Nonetheless, the ability to claim ownership over the aforementioned assets is preceded by the need to access the profile where such "goods" are stored to exercise the deceased's (potential) last will. Post mortal privacy, although not being always a well-grounded or founded concept in data protection, can be achieved by exploiting different "legal paths" such as inheritance law, or under less formal ones that can potentially reconcile the need of post mortal safeguard in terms of right to personal dignity of the deceased without neglecting the primordial need and right to remember however family members or other interested parties may consider appropriate. This balancing exercise leads to the inevitable reconsideration of how online privacy is conceived when two apparently antithetic dimensions (Publicly Forgetting/and Privately Remembering) collide.

First of all, it shall be understood how the afore-presented dimensions may coexist and the clash between the right to be forgotten and to remember unfolds.

> […] At present, there is an increasing call for the protection of privacy and private sphere of the individual, expressed strongly on the level of protection of personal data […] [as] private entities are increasingly making significant, widespread, and extensive intrusions into the private sphere, especially in concerning the traces we leave in the digital world. (Čtvrtník, 2023, *pp*.126)

The contemporary digital environment has for some time been characterized by a quasi-pathological craving for personal information and tracking. Far from being, usually, a malicious intent but rather a trade-off for the "free" offering of digital (personalized) services. As users rely on personalization to navigate cyberspace, they (we) have grown acquainted with the idea that somehow, we are trading our data – our privacy – in exchange for instant gratification and services. As this has a utilitarian connotation in life, that legitimizes the trade-off between privacy and "publicy," the same cannot be said about the afterlife where data and digital assets, in absence of clear disposition, live forever uncontrolled.

As noted, data subjects have the faculty to express their will to have their digital trace erased from social media. As conceived in Art.17 of the GDPR exercising this right leads to the complete deletion of any personal information or content that a controller and processor might have stored about the data subject. Applying said right *as-is* appears to be in blatant contrasts to the legitimate need to "maintain" the digital trace (identity) left by the deceased, so to allow the setup of an online memorial to ease the bereavement process. At first glance solving this peculiar issue could lead to thinking that one party's interest must be overridden, that being either the dead or the living. But looking at the issue from different perspectives could potentially lead to a radical re-framing of the right to be forgotten. According to Čtvrtník (2023) the right to be forgotten is not a monolithic entity but can be divided into four sub-dimensions that can be named and ordered according to their strength in terms of user accessibility and time.

1. "**permanent absolute"** right to be forgotten
2. "**permanent limited**" right to be forgotten
3. "**temporary absolute**" right to be forgotten
4. "**temporary limited**" right to be forgotten (*ivi*, pp.130)

The first dimension corresponds to the right to be forgotten in the meaning of the GDPR, therefore a complete and non-reversible deletion of data and information about the data subject. The second one shifts towards a limited access approach, meaning that it features a weaker level of protection if compared to the "pure interpretation of Art.17": whilst being stronger than the temporary limitations (3. and 4.) or their total absence. This newly established middle ground between privacy and publicity could be defined as *meta-privacy*.

For the sake of analyzing *meta-privacy* and its application to the online afterlife and postmortem data protection the *permanently limited right to be forgotten* (Čtvrtník, 2023) could, as a matter of fact, feature a reasonable "protection of personality rights and the protection of the private and intimate sphere [from the public]"; (*ibidem, pp*.132) while maintaining the ability of the living to "privately and digitally remember the deceased". Keeping this into account, it is possible to reconsider the conception and application of the right to be forgotten within the concept of *meta-privacy*; theoretically setting the path for the re-creation of the close/intimate sphere where a close circle of "selected" individuals - namely family members and friends- fall under.

Recreating said “social space” within the internet and data domain, together with the ability to exercise control over the deceased digital identity might be the closest attempt at bringing digital legacies out of the public and into a substantially private (and self-sovereign) digital domain. As such, meta-privacy is not an abstract concept but rather an operative and technologically enabled (data and identity) governance tool. This last element opens up the discussion whether or not it is possible to envision alternative an innovative way to reconcile the different nuances of the deceased will, the right and need to be -and being-able to remember whilst allowing heirs to effectively being in substantial control of their beloved one’s digital legacy within a secure and self-sovereign digital environment. The conceptualization of a layered data access model able to render information publicly (externally) unavailable and privately (internally) available whilst fostering the setup of a self-sovereign data regime to help overcome the afore-introduced difficulties in dealing with data in the afterlife. In the next chapter the model will be discussed in greater detail as a potential solution to not only enforce meta-privacy but further grant that the stored information will not accidentally be lost.

Chapter Six: A business Proposal in the Digital Afterlife Industry (DAI)

6.1 Defining the DAI sector.

Before discussing the concrete conceptualization of a digital afterlife identity management system, it is mandatory to understand and define the general market and sector. Floridi and Öhman (2017) described the Digital Afterlife Industry (DAI) as “an umbrella neologism that covers commercial enterprises that monetize death online.” (Öhman, Floridi, 2017, *pp*. 643). To fall under the DAI category three criterions must be respected (*ibidem*):

1. **Production**: In order to be classified as an industry, some form of good or service needs to be produced. Thus, the DAI only refers to activities of production, which distinguishes it from activities without a productive outcome such as private, unrecorded grief.

2. **Commercialism**: Firms operating within the DAI produce goods, services or experiences (such as grief or closure) for the purpose of making profit, dealing with what they produce as commodities. This excludes non-profit activities such as religious communities and self-made memorial sites, and also charities that, despite being productive (first criterion), do not make profit.

3. **Online usage of digital human remains**: This refers to any informational content left by the deceased online and distinguishes the DAI from three other types of industries: (1) commercialisation of physical funerals and offline digital activities, such as recorded audio messages and shifting images on tombstones; (2) biological immortality projects that enhance the durability of the organic body; and (3) businesses that deal with digital remains of non-human animals.

This categorization attempt does not only serve as a potential guidance instrument to investigate and research this somewhat unknown branch of digital services, but additionally legitimizes the former under a sociological, legal, technological and psychological light.

6.2 Established services, tendencies and the future

Concretely, Öhman and Floridi (2017) propose an internal subdivision based on the nature of the offered service/product.

a) Information Management Services: Services that help users deal with problems regarding digital asset management that may arise because of their own or someone else's death. Usually, they allow to encrypt relevant information, offer secure storage or set out instructions for the automatic transmission of online credentials to designated heirs. These may include Digital Asset Management Services (DAM)

b) Services that, upon the death of the user, deliver online messages or other digital communicative content to appointed recipients.

c) Online Memorial Services: Services that provide an online space for a deceased individual or group to be mourned and/or remembered.

d) Re-creation services: Services that use personal data in order to generate new content replicating a dead person's social behavior. (*ivi*, *pp*. 645-647)

It shall be clarified that this categorization is highly dependent on the Value Proposition each service is offering to the market, meaning that a given DAI service can factually fall simultaneously in one or more of the above listed categories.

In chapter 4 a series of practical applications and governance tools, deployed by the main social media players, have been listed so to frame a considerable portion of possible solutions for the afterlife management of digital identities. What becomes clear in hindsight, is that these kinds of proposal reflect the substantial tendency of private social media platforms to "lock in" users and their profiles even after death by providing the necessary "toolbox" to memorialize the profile whilst maintaining its content inside the platform ecosystem; thus, the choice to allow for their memorialization appears to some as an egoistic alternative to their deletion. (Krappi, 2013). In parallel, and sometimes well before Facebook's mass adoption, digital memorials have been reported to be around as late as 1995 such as Cemetery.org[33]. Over the last decades many more have found their space in the industry with innovative yet grotesque implementations, such as the ability to recreate a chat with the deceased.

[33] https://cemetery.org/

6.3 Points of Parity and Difference:

Services such as cemetery.org therefore present a series of analogies with the memorialize function offered by Facebook if the core service is being considered. Starting to look at the core business, Facebook is a social network intended to bring people (living ones) together, the presence of “dead” profiles and subsequent necessity to provide a solution to manage the latter could be considered as the “natural” and logical consequence of people being increasingly connected and reliant on intermediated digital communication tools. This leads to consider, as stated by Krappi (2013) that Facebook and similar service providers tend to lock their users in for life. Applying the afore-introduced categorization of the industry, Facebook’s offering would fall under the online memorial service (c). Said memorial function is, and remains an accessory add-on, a service extension of the original offering that allows to conclude that Facebook is not a DAI-native service but rather bares a certain interest to maintain control over ex-user (i.e., nonliving ones) even if the afterlife. Conversely to Facebook, DAI-native services such as cemetery.org find the online afterlife their sole scope of existence and thus, are exclusively committed to a specific service offered within a specific digital space.

6.3.1 Business models

A further key difference emerges upon consideration of the selected business model (BM); Facebook is a free SNS that relies mainly on data processing for personalized advertising to generate income, making the latter a data-intensive platform service provider. DAI-native services, contrary to the adoption of similar models privileges the adoption of *freemium*[34] or subscription-based Business models through which they generate their income. Upon considering different service offerings a commonly exhibited trait where the offered subscription tiers combine features with payment frequency, meaning that free or monthly subscriptions are more restricted while the so-called lifetime plans – whose cost can exceed 100 USD – feature the complete service package.

[34] Freemium models feature two or more service “tiers” that provide access to more or less features depending on the selected subscription plan. The lowest tier which features the greatest limitations is free of charge; additionally, an intermediated and “Premium” service can be included.

6.3.2 Service offering

Service-wise, Facebook's memorization function and dedicated sites, such as the afore-considered one, provide a way to digitally "crystallize" someone's digital identity by posting and sharing multimedia content, including images and text files. Once a memorial account is created on Facebook, the picture therein will still be visible for family and friends to interact with them. Similarly, yet under a different (more specialized) light, DAI-native services allow family members to set up a "memorial space" where everyone can express thoughts and share images or memories about the deceased. In some cases, "visitors" can purchase a digital candle or similar digital goods to "pay a tribute." Few differences can be highlighted in terms of concrete service offerings.

6.3.3 Security measures

Looking briefly at the information security aspect of memorial services may come in useful to better understand the concerns and risks at stake. Particularly DAI-native websites require the creation of a profile to access the service and similarly family members and friends are required to create a profile to interact with the memorial; other times the interaction capability is free of registration thus, allows anyone that visits that particular memorial to post "something" even potentially detrimental to the deceased personality and/or dignity. In this sense public exposure becomes a wider concern as the personal data of the deceased (name, surname, date of birth (sometimes also including day and month), birthplace, and other relevant information are all publicly visible. Facebook's memorial account function has been already object of discussion in chapter 4.3.2 thus, it suffices to briefly consider and highlight that, conversely to DAI-native services, memorial accounts within Facebook get their visibility and searchability limited to the contacts the person already had in life. This need for separation is not only required to avoid sparking unnecessary confusion between the dead and the living that coexist on the platform, but also to avoid harming the sensibility of immediate family members and friends during the bereavement process. Among the many changes the memorialization of a Facebook profile makes is disabling birthday and other update notifications about the dead.

> Unless Uncle Jimmy died two years ago, and his far-removed co-workers are still flooding your newsfeed with confetti emojis and well-wishes for him. Nothing ruins a day like a notification to wish your dead relatives a happy birthday. It’s an uncomfortable reminder that while man is still mortal, the internet lives forever. (Andrews, 2019)

> While some users may find the online profiles of dead people disturbing, anecdotal evidence suggests that memorialised profiles can be helpful for those in grief, by enriching their engagement with their memories of the deceased and with others who knew them. [The profile itself becomes therefore a repository for digital memories that can -as already proven- be compared to diaries, printed photos or other analog contents]. […] Memorialised profiles offer a suite of visual and textual resources to assist the memories of the survivors—not in the sense of helping someone not forget the dead, but in phenomenally enhancing the experience of remembering the dead. For one engaged in the act of remembrance, these visual and textual resources can provoke Proustian rushes of rich involuntary memory, or affirm, reinforce or correct existing memories. They thereby assist the phenomenality of the dead in persisting in the memory of the living. (Stokes, 2012, *pp*. 367)

Having assessed the necessity to find “innovative ways” to express and cope with grief the implications the use of technology to set up a memorial has inevitable and non-neglectable consequences in the domain of personal data and personal dignity of the deceased. Current market trends appear to feature some degree of protection, mainly by encrypting information or featuring the ability to selectively make memorial pages selectively available. Despite the deployed security measures, the fact that such important and sensitive information is stored on third-party servers exposes the deceased digital identity to general cyber-risks, loss of data as well as substantial lack of direct control.

It could even be said that data sensitivity of this services requires a greater level of security and dignity that cannot be achieved by “uploading the dead on a public website.” The possibility to adopt disruptive technologies working towards achieving *meta-privacy* as previously described might foster innovation in the DAI sector whilst reconciling the need for substantial and long-lasting postmortem information security with the ability to express grief and find closure through digital services.

6.4 Why caring for digital identities and assets: Bit Rot & Digital Vellum

Digital assets and identities have an undeniable social role and value in contemporary society. The very concept of value can be considered as purely economic/financial (monetary value) as well as emotional value. Especially considering, as reiterated over the previous chapters, the role of social media and personal self-communication our personal profiles can be considered as true repositories of our online and offline existence. To further ground this affirmation, it suffices to consider how some social media platforms feature a post archive that allows the user to display when and where a particular story[35] or post was created; effectively creating a digital interactive album.

As this appears to be sufficient by some, the risks of account hijacking, data loss our service takedown endangers the very existence and availability of these assets and identity "particles." Concretely speaking, if a social media platform ought to suffer a major cyber incident the users will not be able to access their profile making it exceedingly difficult to retrieve copies of the posted contents.

> Web 2.0 may not be the hot young topic it once was, but it still hasn't been around long enough for us to figure out questions around long-term, and legacy data storage. […] The data stored on legacy systems will either be useless, or deleted along with the platforms (Indriya, 2017)

This remote yet possible scenario if not addressed could doom current society to *bit rot*. "Bit rot refers to the irrevocable degradation or loss of digital information when the infrastructure (the hardware and software) required to access, interpret, view, and use this information is no longer available or executable" (Kosciejew, 2015, pp.21). Bit rot therefore affects digital information as well as the enabling technological infrastructures, radically dimensioning the idea(s) around the default perpetual existence and availability of digital contents online. When presenting digital immortality, it has been said that digital identities systematically outlive biological existence since they can "virtually live forever." Introducing Bit rot as a variable it becomes clear that such a statement is partially correct and further measures must be taken to truly strive towards digital immortality as its achievement appears to be far more complex than simply crystallizing – for example- a social media page. Without any measures taken, or better leaving things as-is,

> We are nonchalantly throwing all of our data into what could become an information black hole without realising it. We digitise things, [even ourselves] because we think we will preserve them, but what we do not understand is that unless we take other steps, those digital versions may not be any better, and may even be worse, than the artefacts that we digitised." Ironically, the very black hole we fuel with our data and ourselves might become a digital *oubliette* rather than an archive.

[35] Stories are temporary posts that upon creation will have a 24-hour visibility period. After the time is expired the creator (owner) will still be able to view or repost them.

Vint Cerf, one of the founding fathers of the TCP/IP protocol, declared that containing bit rot is possible through various approaches, among the many Cerf mentions – such as hardware and software preservation to grant future accessibility and availability- it is noteworthy to focus on the idea of Platform diversification. By making several digital copies of information accessible in various places and applications, platform diversification may also assist in lessening the impacts of bit rot. Digital copies do not decay concurrently because bit rot affects various hardware and software at different periods - everything degrades at a different rate. By giving more time to plan and put methods in place to manage bit rot before and when it arises, creating digital copies for various platforms can aid in the preservation of data and digital assets.

The many different approaches to mitigate *bit rot* can be comprised under the concept of digital Vellum that Cerf used to explain the necessity to envision solutions to not only preserve hardware and software but maintaining a comprehensible trace of their functioning and operational requirements by concretely explaining how they used to work. Digital Vellum is therefore one of the possible "cures" for bit rot and avoiding the total loss of data and digital assets in a world exceedingly dependent from third party hardware. Since the creation of a digital Vellum can start from the diversification – and storage decentralization – of digital contents it is reasonable to argue that applying blockchain technology beyond the mere protection of personal data and information in the afterlife can theoretically address the increasingly pressing issue of losing substantial access and availability of those data that people might be willing to safeguard over time. "Taking some of these steps today can help tomorrow remember. We do not have to become a forgotten generation. Planning and preparing for bit rot can help ensure that we are and remain a remembered generation" (Kosciejew, 2015, *pp*.25).

6.5 A legacy blockchain:

Upon analyzing different services who exhibit an affinity with the DAI sector a memorial centered tendency emerges; in layman's terms meaning that most of the time they exclusively focus on creating a digital (open) shrine to celebrate the deceased. While doing so the concern for the deceased data, information, contents, and digital assets in general is not prioritized if not partially delegated to different service offerings such as information management services that specifically focus on managing profiles and online contents.

Considering the relevance of data and personal information, to a certain extent digital assets also have in cyberspace and society, their safeguard shall become a *sine qua non* requirement. It can be argued that currently both Facebook and other services take care of this aspect by implementing encryption algorithms and other information security protocols or policies.

Albeit true, these (grief) manifestations still happen within and through the public cyber environment or even worse require, even after death, the intermediation of a third-party service provider. Another shortcoming of third-party mediation is that data are stored on proprietary servers that might at any moment fail, or lose data all together; in other words, no centralized server or storage is fail-proof nor bit rot-resilient. Beside this remote possibility, the fact that a considerable part of individual and collective memory is not in substantial possession should be a first signal for users to consider different means of online storage solutions.

It shall be therefore reasoned if, in the light of the intrinsic complexity the online afterlife brings to the discussion, meta-privacy can act as guidance in the creation of an innovative and integrated digital identity (or asset) management tool that can ensure long-term data and information resilience. Meta-privacy has been previously introduced as a new-found conceptual and operational element applied to the re-creation of a private and controllable space away from the internet's publicity; allowing to reconcile a series of different needs and concern mitigation that all find a common root in data and information being widely available and at public display. On more than one occasion the hypothesis to leverage blockchain as a way to create a secure digital memorial ecosystem thus enabling the creation of a personal digital vault (or Vellum) to be passed on to future generation has been advanced. Consequently, it becomes necessary to understand concretely how blockchain can:

a) Provide the necessary safeguards to protect the integrity of one's digital identity in the afterlife, among the many from bit rot.
b) Allow heirs to substantially exercise direct ownership and control over postmortem digital assets.
c) Reconcile the possible need/request of the deceased to be publicly forgotten and privately remembered (meta-privacy).
d) Preserve the personal identity in respect of the deceased personal dignity and integrity.

The governance and security advantages of a permissioned blockchain environment, together with the substantial ability on the user side to self-determination and self-sovereignty over the wallet’s content translates into the concrete possibility to create a private asset identity vault whose management, including inheritance, can be easily and directly be controlled by the wallet holder, in brief a permissioned blockchain can allow for the creation of a private digital space within the wallet (private memorial vault) entirely based on the concept of *meta-privacy*, keeping in mind the need to mitigate the risk of *bit rot* and generational digital oblivion as much as possible.

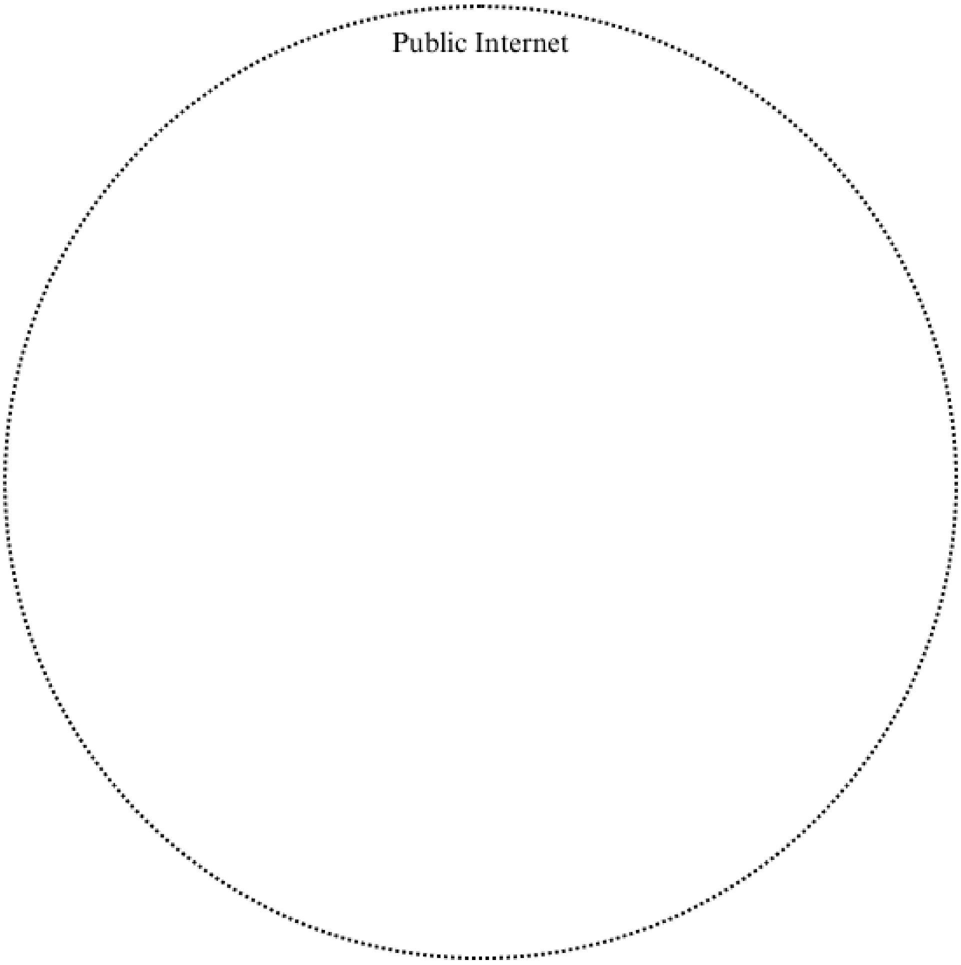
6.5.1 Layered access model

Applying blockchain technology to the data domain comes with a series of crucial negotiation moments that affect the very conception of privacy and data protection rights at large. If one of the informal rules of the internet states that "once something enters the internet, it is hardly forgotten" within a blockchain environment, this is not only a definite possibility but a mandatory system requirement. The feature of perpetual archiving can be problematic when thinking about data rights of the living and the subsequent application of DLT to access and identity management solutions. This negotiations attempt appears to be simpler, if not somewhat predetermined- if applied to the management of digital identities and assets of those who want to "live forever" online while avoiding sacrificing their dignity, safety as well as legacy transmissibility while acknowledging the risk that at some stage "bit rot" might lead to the unavailability of digital information at large. Considering the technological requirement for long-term memory in a different light, it can already be seen how blockchain, by design, features a strong tendency to avoid data loss over time, as every previously created block is essential to sustain the scaffolding of the entire protocol. Furthermore, blockchain being a Distributed Ledger Technology (DLT), it already incorporates the afore-introduced digital vellum solution by decentralizing and diversifying where data are stored (Platform diversification).

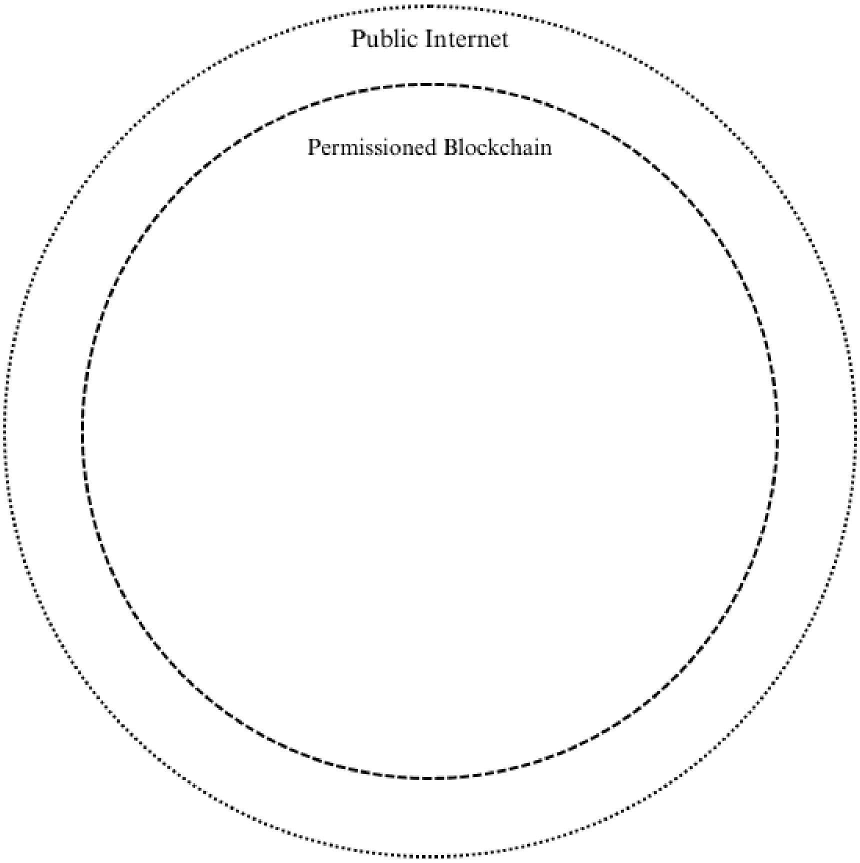
To better understand and accompany the explanation about the advantages of blockchain environments applied to memorialization and online identity and asset management, a *layered access model* has been elaborated. The aim of said model is to explain how blockchain serves and fosters the endeavor to simultaneously apply meta-privacy and bit rot resistant practices into a potential real-life application.

Each circle represents a possible action space with different functions and features. The size of each circle and the line pattern, respectively, reflect the size of the considered space and the restriction potential that subsequently applies; the more solid the line gets, the higher the degree of control and closure that applies to the selected environment.

Data, identities, and assets in the public internet domain are potentially accessible and so vulnerable to a wide array of cyber risks and complete unavailability over time. With an analogy, trying to keep digital assets secure through a website or a memorial page is as safe as keeping valuable goods in a clear and unlocked “vault” where everyone can see or interact with the stored content. Besides exposure, the “content” suffers from being uploaded on “some” third-party server, thus exposing the stored information and assets to permanent loss (bit rot) in cases of major incidents or service discontinuation. A further negative spillover comes with the decreased capability of owning and controlling the affected digital assets in a complete and direct manner independently from the server and service availability. According to Cerf: “All web users are at risk of throwing their data away into a "digital black hole" in the mistaken belief that uploading content to a site or service will preserve it (Donnelly, 2015).

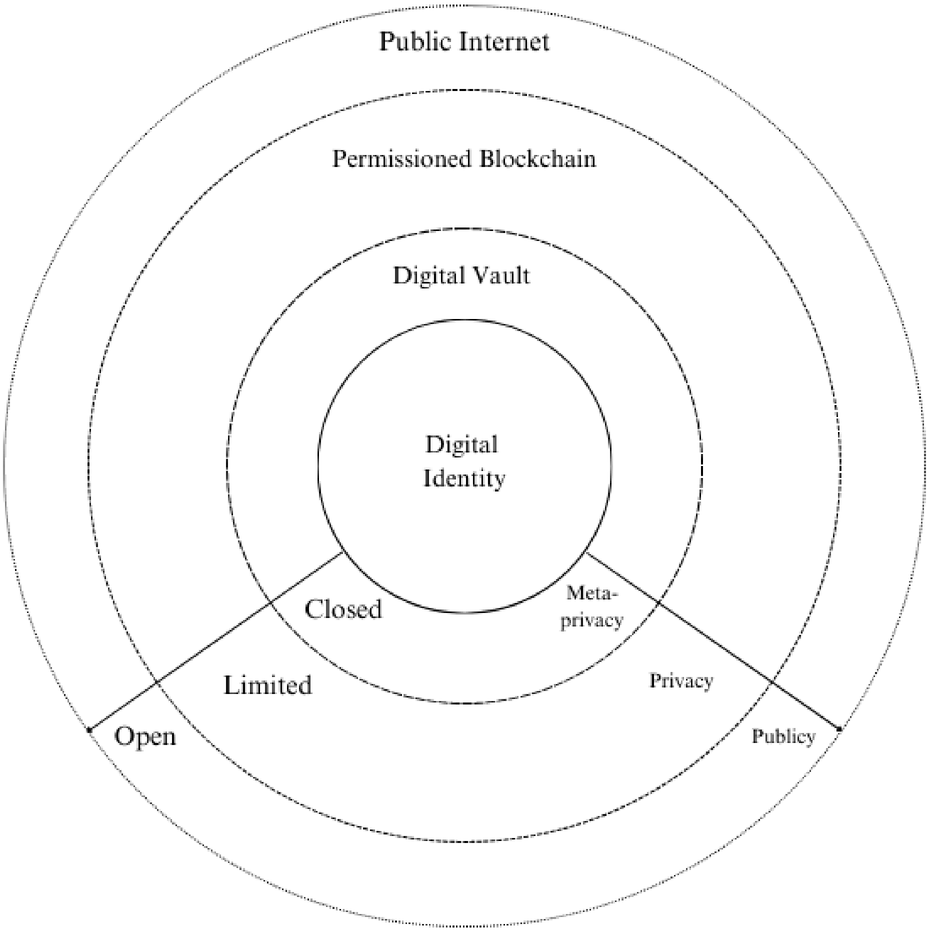


The scenario gradually changes when said digital assets are no longer uploaded on some server but stored within a decentralized architecture. The advantages of decentralized storage architectures have already been discussed, underlining their resiliency and tamper resistance. Permissioned blockchain environments (see 1.2.2) are, by protocol, a closed system of verified nodes comprised within a selectively accessible environment. This first "security layer" forms a first entrance barrier for external (non-authenticated and authorized parties. Considering this, the information that enters the permissions architecture is invisible for many on the outside and visible for the few on the inside. Depending on the architectural and service features data and assets might require additional protection measures in the form of encryption.



Enabling users to request the deletion of all information (*right to be forgotten*) while maintaining them "alive" within an access-limited digital space as theorized while explaining the *ratio* behind Meta-Privacy. Within the distributed architectures, i.e., permissioned blockchains, users (i.e., wallet owners) can store assets within their wallets. Once a user owns a given asset, it is stored inside a wallet and becomes exclusively visible and fungible by that particular wallet owner. Therefore, at the discretion of the wallet owner, access to the information can be controlled/moderated, for instance, by opening or further restricting their availability. The digital vault is not only the main "data gateway" but constitutes the concretization of a truly digital private sphere as formalized in the meaning of meta-privacy. Not only that, DLT technologies, as already discussed, can be organized as peer-to-peer (P2P) systems meaning that users are truly in possession of their vault and its content.

Beside the evident advantages deriving from direct data ownership and controllability it is evident that a Digital Asset Management designed to incorporate said model could be the first step towards rethinking towards a more aware, secure and affordable digital asset management solution empowering users in an already uncertain and difficult part of their life.



6.6. Personal Digital assets and the global common(s) cyber-culture:

Individually “prepping” for bit rot through the use of a possible blockchain-based archive solution originates from the individual need to leave something behind. Considering the hypothesis that bit rot may lead to the global oblivion of everything created and stored online it becomes evident that the issue around digital oblivion has wider implications beyond the individual dimension. The internet is populated by spontaneously created contents that tell a story about the creator or provide an insight about his view. These individual contributions appear, in a bottom-up perspective, to create a personal yet shared cultural production that happens and exists within the boundaries of the internet. Filtering this assumption through the lenses of Ostromian governance and the principle of *commons* (1990), it is reasonable to start thinking about cyber-culture as a collective co-creation of public and private digital assets.

Factually, each user that has ever interacted or created something online has contributed to the creation of a small fraction of global cyber culture; this would imply that, theoretically the global cyber-culture can be expressed as a continuous common co-creation effort partially owned by each participant. Digital assets have been described as the “bricks” that make up digital identities, but within the wider frame of cyberspace they become digital commons or “a subset of the commons, where the resources are data, information, culture and knowledge which are created and/or maintained online” (Dulong, Stadler, 2020, *pp*.1).

This consideration would imply that by individually securing an individual portion of one’s digital identity and assets, a small portion of the collective internet culture is also being secured from rotting away. Hence, leading to the conclusion that the sum of individual heritages can potentially be a way to not only pass individual but also a more or less consistent part of the collective digital heritage, to future generations; effectively leaving a larger testimony that otherwise would get lost.

Conclusions

The expansion of private and public self-narration practices through the internet and social media has radically reshaped how individual and collective memory are created online and offline. The creation of memories through User Generated Contents simultaneously leads to the additive construction of a digital repository that not only tells something about the narrator (the user) but constitutes its "digital presence" or identity in the form of data and other personal digital contents. Digital identities have been proven to be a multiformat and faceted entity that covers a crucial role in life but has considerable importance in the afterlife and foreseeable future.

As digital identities and assets systemically outlive biological existence, enabling users to become digitally immortal, it is sometimes unclear how to manage the rich and pluralistic content that constitutes them. To better understand the fate of data and digital assets in the afterlife, looking at data protection and civil law has allowed us to conclude that despite such data and contents usually not being protectable equally to personal data of the living, they can be inherited and consequently turned into digital assets.

It was possible to conclude that the *de cuius* (the deceased) could express their will about the post-mortal management of their digital asset. The *de cuius* mandate can be broken down into two general categories: being either remembered (through the use of online services) or having their online presence completely deleted. The concrete and theoretical clash between the right to be forgotten and the right to remember has finally led to the conceptualization of a possible solution, originating from reconsidering the right to be forgotten not as a monolithic entity but as a more nuanced and dynamic one.

Through the concept of meta-privacy, the two afore introduced opposite dimensions have been possibly reconciled by considering the possibility of leveraging blockchain technology to recreate a digital space resembling the intimate offline private sphere, enabling the data of the de cuius to be permanently archived in a non-public yet privately accessible environment for those wishing to uphold or maintain the digital legacy "alive." At the same time, providing a solid theoretical and potential ground for the setup of innovative services in the digital afterlife industry (DAI) by combining the classic functions of digital memorials with an enhanced level of data security and ownership of Digital Asset Management services (DAM)

Knowing that secure and fail-proof (or bit-rot-proof) storage services exist could lead to a radical reconsideration of data privacy, the right to be forgotten and remembered. Simultaneously addressing the problem that long-term data storage solutions must be bitted rot resilient to ensure that all efforts of those wishing to preserve a considerable and rich contribution to the global cultural digital heritage will not be unnecessary. The increasingly relevant value of personal data and information shall lead users to at least start to consider what to do with their digital identity and assets after their death, possibly even giving instructions or taking the initiative to create a personal digital vault.

At first sight, governing digital assets, and ensuring their protection and inheritability after the owner's death, appears to be an individualistic decision solely affecting the de cuius and a few close people. In reality, considering the complexity and exponential interconnection between single users, ensuring that digital assets resist the tendency to rot digitally has a broader meaning and importance for preserving our collective digital heritage. Committing to individual digital immortality through blockchain technology is an altruistic contribution to create a global cultural repository that every user at any given moment participates in and is involved in from the moment when they join cyberspace. Global internet culture is the richest and most pluralistic testimony of human intellectual activity while being one of the most fragile and difficult to preserve.

Memory, oblivion, privacy, and publicity can no longer be considered static, immutable, non-dialogical, and non-negotiable elements or rights; they can -and must- be re-combined and made compatible; by applying the right technology in the right way, potentially overcoming the barriers and shortcomings of traditional technological solutions to keep on existing and "living" in cyberspace. As a final word, this thesis started with the aim to address the issue of personal data and information security in the afterlife, considering the possibility of leveraging technology to provide an enhanced degree of protection and control over digital assets in the online afterlife. The role we, as citizens of the global internet, have overcomes and expands beyond the individual need or will to leave something behind or ensure that our data will flow smoothly in cyberspace. Every user, with no discrimination whatsoever, can make his existence matter. The survival of our digital heritage (as humankind) can be considered the result and consequence of the individual will and need for digital self-preservation. In a certain way, diligently fostering the integration of new technologies and law data protection not only leads to a deep reconsideration of data protection and online security in the afterlife, but it also sustains the collective cultural endeavor to leave something behind, a testimony of our time. Failing to innovate the legal frameworks in the governance of internet end technology stunts the emergence of competitive markets and economic growth. Further, it complicates the individual and collective endeavor NOT to be forgotten.

"[If] we don't want our digital lives [and collective existence] to fade away. If we want to preserve them, we need to make sure that the digital objects we create today can still be rendered far into the future."

– Vint Cerf, Vice President at Google.

Bibliography

„Digitaler Neustart “, 2017, https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf (15/05/2017)

Andrews, J. (2019). *Still getting Facebook birthday reminders for your dead relatives? Here's the new solution*. (2019, July 24), CNBC, https://www.cnbc.com/2019/07/24/facebook-still-highlighting-dead-relatives-birthday-heres-solution.html (Accessed, 08/05/23)

Bacchi, U., 2020, Data of the dead: Virtual immortality exposes holes in privacy laws. (2020, April 17). Reuters. https://www.reuters.com/article/us-global-tech-privacy-trfn-idUSKBN21Z0NF (Accessed, 08/05/23)

Bentivegna, S., Boccia Artieri, G., (2019) , Le teorie delle comunicazioni di massa e la sfida digitale, Editori Laterza, Bari

Boyd, d.. (2010). Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In Networked Self: Identity, Community, and Culture on Social Network Sites (ed. Zizi Papacharissi), pp. 39-58

Brubaker, J. R., Hayes, G. R., & Dourish, P. (2013). Beyond the Grave: Facebook as a Site for the Expansion of Death and Mourning. The Information Society, 29(3), 152–163. https://doi.org/10.1080/01972243.2013.777300

Castells, M., (2007), Communication, Power and Counter-power in the Network Society. International

CNIL, (2018). *Solutions for a responsible use of the blockchain in the context of personal data*, https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

Corona, G., (2017), Eredità digitale: La tutela dei dati digitali dopo la morte. (2017, maggio 3). Altalex. https://www.altalex.com/documents/news/2017/05/03/eredita-digitale-la-tutela-dei-dati-digitali-dopo-la-morte

Čtvrtník, M. (2023). Archives and Records: Privacy, Personality Rights, and Access. Springer International Publishing. https://doi.org/10.1007/978-3-031-18667-7

D'Acquisto, G. (2021). Blockchain e GDPR: Verso un approccio basato sul rischio. (s.d.). Recuperato 9 febbraio 2023, da https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=44784&dpath=document&dfile=18012021003517.pdf&content=Blockchain%2Be%2BGDPR%3A%2Bverso%2Bun%2Bapproccio%2Bbasato%2Bsul%2Brischio%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B

DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174) https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29

Donnelly, C. (2015). *Google VP leads calls for web content preservation*. ITPro, (february 13th, 2015) (https://www.itpro.com/strategy/24047/google-vp-leads-calls-for-web-content-preservation (Accessed: 16/05/23)

Dulong De Rosnay, M., & Stalder, F. (2020). Digital commons. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1530

Facebook ruling: German court grants parents rights to dead daughter's account. (2018, July 12th). BBC News. https://www.bbc.com/news/world-europe-44804599

Finck, M. (2018). Blockchains and Data Protection in the European

Garde-Hansen, J. (2009). My memories?: Personal digital archive fever and Facebook. In J. Garde-Hansen, A. Hoskins, & A. Reader (Eds.), Save as...: digital memories (pp. 135–150). Hampshire: Palgrave. https://doi.org/10.1057/9780230239418_8

Gesley, J. (2018) Germany: Federal Court of Justice Rules Digital Social Media Accounts Inheritable. [Web Page] Retrieved from the Library of Congress, https://www.loc.gov/item/global-legal-monitor/2018-09-07/germany-federal-court-of-justice-rules-digital-social-media-accounts-inheritable/.

Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape social media. In Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media (p. 288). https://doi.org/10.12987/9780300235029

Gonçalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: A critical perspective. Journal of Risk Research, 23(2), 139–152. https://doi.org/10.1080/13669877.2018.1517381

https://cemetery.org/ (Accessed 17/05/2023)

https://consensys.net/blockchain-use-cases/digital-identity/ (Accessed 17/05/2023)

https://ethereum.org/en/decentralized-identity/ (Accessed 17/05/2023)

https://help.twitter.com/en/rules-and-policies/inactive-twitter-accounts#:~:text=What%20is%20Twitter's%20inactive%20account,removed%20due%20to%20prolonged%20inactivity. (Accessed 12/05/23)

https://support.google.com/accounts/answer/3036546?hl=en&sjid=1869111665463341259-EU (Accessed 15/05/2023)

https://www.facebook.com/help/1111566045566400 (Accessed 14/05/2023)

https://www.facebook.com/help/991335594313139 (Accessed 14/05/2023)

https://www.facebook.com/help/contact/234739086860192 (Accessed 14/05/2023)

https://www.grandviewresearch.com/press-release/global-blockchain-technology-market (Accessed 10/04/2023)

https://www.statista.com/statistics/1015362/worldwide-blockchain-technology-market-size/ (Accessed 18/03/2023) https://www.twobirds.com/en/capabilities/practices/privacy-and-data-protection/general-data-protection-regulation/gdpr-tracker/deceased-persons (Accessed 20/03/2023)

III ZR 183/17 https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2018-7&Sort=1&Seite=4&nr=86602&pos=142&anz=302

Indriya, O., *(2017), (6) Do You Know Where Your Photos Are? (Really? Are You Sure?)* | *LinkedIn*. (n.d.). from https://www.linkedin.com/pulse/do-you-know-where-your-photos-really-sure-osiris-indriya/ (Accessed: 16/05/23)

Karppi, T. (2013). Death proof: On the biopolitics and noopolitics of memorializing dead Facebook profiles. Culture Machine, 14. Retrieved from: www.culturemachine.net/index.php/cm/article/ download/.../528.

Kelly, M., (2009), Memories of Friends Departed Endure on Facebook, The Facebook Blog 26 October 2009. https://www.facebook.com/notes/10160196742716729/?paipv=0&eav=AfbGcv8dci8t8v22y7dNBI006GAwb3F9dxwOVqWeWFmfLcn34J7uUfMAGskLWdPayKw Accessed 13/04/2023.

Kosciejew, M. (2015). *Digital Vellum and Other Cures for Bit Rot*, in ARMA Information Management, May/June 2015

Lessig, L., (1999). *Code: And Other Laws of Cyberspace*, Basic Books

Lamport. L., (1998). *The part time parliament*, in ACM Transactions on Computer Systems 16, 2 (May 1998), 133-169.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article85

Malgieri, G., (2018). *R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions* (March 30, 2018). Data Protection and Privacy: The Internet of Bodies, edited by Ronald Leenes, Rosamunde van Brackel, Serge Gutwirth & Paul De Hert (Brussels, Hart, 2018), Available at SSRN: https://ssrn.com/abstract=3185249

Marino, G., (2018). *La «successione digitale». Osservatorio del diritto civile e commerciale*, 1, 167–204. https://doi.org/10.4478/90680

Mayer-Schönberger, V., Cukier K. (2013). *Big Data: A revolution That Will Transform How We Live, Work and Think*, Houghton Mifflin Haracourt, Boston.

Öhman, C., & Floridi, L. (2017). *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*. Minds and Machines, 27(4), 639–662. https://doi.org/10.1007/s11023-017-9445-2

Ostrom, E. (1990). Governing the Commons. Cambridge University Press.

Pino, G., (2000). *The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights*, [in The Harmonization of Private Law in Europe, edited by M. Van Hoecke and F. Ost, Hart Publishing, Oxford, 2000, pp. 225-237.]

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

Riva, G. (2016). *I social network,* 2. Ed., il Mulino, Bologna.

Romanov, A., Semenov, A., Mazhelis, O., Veijalainen, J., (2017). *Detection of Fake Profiles in Social Media - Literature Review:,* in: Proceedings of the 13th International Conference on Web Information Systems and Technologies. Presented at the 13th International Conference on Web Information Systems and Technologies, SCITEPRESS - Science and Technology Publications, Porto, Portugal, pp. 363–369. https://doi.org/10.5220/0006362103630369

Schumpeter, J. A. (1942). *Capitalism, Socialism and Democracy,*

Ziccardi, G., (2017). *Il libro digitale dei morti memoria, lutto eternità e oblio nell'era dei social network*, Utet