PROTECTION OF PERSONAL DATA THROUGH IMPLEMENTATION OF THE RIGHT TO INFORMATIONAL SELF-DETERMINATION: IDENTIFYING OPPORTUNITIES AND PITFALLS

TATIANA SHULGA-MORSKAYA

C.E.R.C.C.L.E. - EA 7436, University of Bordeaux

2019 ANNUAL GIGANET SYMPOSIUM

25 NOVEMBER 2019 - BERLIN, GERMANY

ABSTRACT

The right to informational self-determination, which foundations in the European Union have been laid by the General Data Protection Regulation (GDPR), aims to strengthen the individuals with regard to the protection of their personal data. The implementation of this right could change the approach to data protection: not only as a set of obligations on controllers and processors, but also as a self-protection of individuals through a set of legal and technical means. However, serious questions arise regarding the capacity of the existing legal framework to allow full implementation of this right. Two case studies – Solid and Self-Sovereign Identity – represent different approaches to its implementation and illustrate the need in further research.

INTRODUCTION

"Users have few if any means to enforce their privacy and personal data-protection rights, even when recognized by legislation."[1] Even after the entry into force of the Regulation (EU) 2016/679 of 27 April 2016 (GDPR), which represents the most advanced legal instrument in the field, some of its rights and obligations remain more theoretical than practical. The situation of the data subjects has not significantly changed so far. At the same time, each action on the Internet creates data and metadata related to the individual that reveal a lot about his or her private life[2]. A reinforcement of legal and technical means is needed, to ensure the protection of individuals' personal data and therefore their private life online.

Three points of view on a privacy-ensuring legal framework for personal data can be identified:

(a) data "ownership", "a proprietary right that seeks economic participation of the data producer in the income generated from the commercialisation of data"[3];

(b) State protection of the residents from misuse and abuse of their personal data, through recognition of a fundamental right to the protection of personal data;

(c) data subjects' self-protection through the right to control their personal data (right to informational self-determination).

The first point of view has been shaped by the U.S. academic discussion and found its implementation in some states of the USA where laws treat certain personal data as a form of property.[4] At the same time, Section 1, Sec.2, (a), of the 2018 California Consumer Privacy Act (CCPA) reads as follows: "In 1972, California voters amended the California Constitution to include the right of privacy among the

[1] Report of the Working Group on Internet Governance (2005). p.7. https://www.wgig.org/docs/WGIGREPORT.pdf.

[2] See, e.g., Judgment of 8 April 2014. *Digital Rights Ireland Ltd.* C-293/12 and C-594/12. ECLI:EU:C:2014:238. http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

[3] DREXL, J., HILTY, R.M., GLOBOCNIK, J. et al. (2017). Position statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public consultation of building the European data economy". Muenchen: Max Planck Institute for Innovation and Competition. p.4.

[4] European Commission. (2016). Legal study on Ownership and Access to Data – Final Report. https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1. p.6.

"inalienable" rights of all people. […] Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information."[5] These provisions seem to introduce in California, where major tech giants are based, the informational self-determination, accompanied with individuals rights for this purpose.

In Europe the possibility of ownership-like rights over personal data has been disputed by legal doctrine[6], while the second point of view is implemented: the right to the protection of personal data is enshrined in Article 16 of the Treaty on the Functioning of the European Union (EU) and Article 8 of the EU Charter of Fundamental Rights. In each Member State there is a data protection authority (DPA) that supervise the application of the data protection law and handle complaints against its violations. However, in the context of permanent proliferation of personal data, State's capacity to efficiently protect its residents might be called into question. The third approach thus seems to be promising. But it would be viable only on condition that the environment, where the individual is supposed to take decisions, changes. In the existing environment - imposed and incomprehensible terms of service, anti-privacy protocols, and business models built on unlimited collection of personal data of users and even non-users of the service - the data subject is not a contract stakeholder but the weaker party, with a considerably restricted freedom of decision.

Informational self-determination appears even more pertinent considering that the concept of privacy seems to be changing in the digital age. From the right to be left alone,[7] in other words, to share as less data as possible, it becomes a right to control own social situation, which means to control what personal information is shared and to build one's image online.[8] From a legal standpoint, the right to respect for private and family life has evolved under the influence of European case-law: protecting

---

[5] Assembly Bill No. 375. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[6] See, e.g., ROCHFELD, J. (2015). Les géants de l'internet et l'appropriation des données personnelles : plaidoyer contre la reconnaissance de leur "propriété", IN *L'effectivité du droit face à la puissance des géants de l'Internet Vol 1 : Actes des journées du 14,15 et 16 octobre 2014*. / BEHAR-TOUCHAIS, M. (ed.). Paris: IRJS éditions, p.73-88. ; OCHOA, N. (2015). Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition. *RFDA*, p.1157.

[7] WARREN, S.D. & BRANDEIS L.D. (1890). The Right to Privacy. Originally published in 4 *Harvard Law Review* 193. https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/the-right-to-privacy.

[8] See, e.g., MARWICK, A. & BOYD, D. (2018). "Understanding Privacy at the Margins." in *International Journal of Communication* (12), 1157-1165.

initially only the intimacy of the person, today it also includes the freedom to choose one's lifestyle and relationships, in other words, self-determination.[9] Some legal scholars argue that the principle of self-determination is to become a general principle of interpretation of the European Convention on Human Rights.[10] Seen from this perspective, a right for everyone to protect his or her own privacy perimeter might become a new vision of data protection: not only as a State's protection of its subjects but as a self-protection of individuals who must have efficient technical and legal means for this purpose.

The question that arises in this respect: Does the existing legal framework for personal data in the European Union allow full implementation of the right to informational self-determination? To answer the question, this paper proceeds as follows. Part I describes the origin and the content of the right to informational self-determination. Part II examines the pitfalls in implementation of this emerging right within the existing EU legal framework, on the example of digital advertising ecosystem. Part III analyses different approaches to implement the individuals' self-determination, their advantages and limitations. Part IV concludes with the necessity of future research in the field and some recommendations on a legal and technical framework, allowing a full implementation of the right to informational self-determination.

PART I – THE RIGHT TO INFORMATIONAL SELF-DETERMINATION: ORIGIN AND CONTENT

Self-protection of individuals against a massive collection and unauthorized use of their personal data requires a set of legal and technical means at the disposal of data subjects. As for legal means, a right to informational self-determination could constitute a legal basis for such self-protection. The German Federal Constitutional Court (*Bundesverfassungsgericht)* was the first to recognize its fundamental character in 1983. It defined this right as "the power of individuals to make their own decisions as regards the disclosure and use of their personal data, [while] restrictions of this right are permissible

[9] HENNETTE-VAUCHEZ, S. & ROMAN, D. (2015). *Droits de l'Homme et libertés fondamentales*. 2e édition. Paris : Editions Dalloz. p.488.

[10] SUDRE, F. (2015). *Droit européen et international des droits de l'homme*. 12e édition refondue. Paris: PUF. p.710.

only in case of an overriding general public interest."[11] In other words, the Court, firstly, recognized that the privacy perimeter could not be defined once and for all. Everyone should therefore be able to define it for themselves. Secondly, the Court empowered the individual to impose own vision of this perimeter on others, including the State.

This milestone judgment was delivered in response to the Government's plan to conduct a German population census. This project encountered a strong opposition in the society, fearing that collected data could be linked to private individuals, especially since there were 160 questions to be answered, which would give an opportunity to build quite detailed profiles. Furthermore, such a database would not only serve for statistical purposes but also allow the authorities to correct the official records as well as to verify the information already available on the individuals.[12] In its judgment, the Court pointed out that, without reinforced protection of personal data, technological development "would not only restrict the possibilities for personal development of those individuals but also be detrimental to the public good, since self-determination is an elementary prerequisite for the functioning of a free democratic society, predicated on the freedom of action and participation of its members."[13]

Practice has shown that the Court's fears were not exaggerated. The "surveillance capitalism"[14] and its business model based on the unlimited collection and processing of user's personal data, allowing building their detailed profiles, have led to the emergence of new surveillance actors: private Internet companies. Together with governmental programs, such a surveillance network might be of concern not only to specialists. The Facebook-Cambridge Analytica data scandal has clearly demonstrated the link between data protection and democracy. The right to informational self-determination could therefore become necessary for the proper functioning of democracy.

Indeed, this right has already been under construction in Europe. Even if the Directive 95/46/CE of 24 October 1995 did not provide for the right to informational self-determination, it established the data

[11] Census Act, BVerfGE 65, 1. Volkszählungsurteil in englischer Sprache: Census Act. Translation by Conrad-Adenauer-Stiftung. 2013. https://freiheitsfoo.de/census-act/.

[12] HORNUNG, G. & SCHNABEL, C. (2009) Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law&Security Review*, 25 (11), pp. 84-88, p.85.

[13] Census Act, *supra*.

[14] ZUBOFF, S. (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), p.75-89.

subject's right to obtain from the controller an access to data relating to the individual, as well as the right to rectification, erasure or blocking of data the processing of which does not comply with the provisions of the directive (Article 12) and the right not to be subject to a decision which is based solely on automated processing of data (Article 15). Furthermore, Article 14 of the directive provided for the right to object "on compelling legitimate grounds relating to the particular situation" to the processing of personal data, in cases where the processing was necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for the purposes of the controller's legitimate interests. The unconditional right to object to the processing of personal data for the purposes of direct marketing and the right to be informed and to object to disclosures of personal data to third parties completed the self-determination "starter package" of rights.

The GDPR, repealing the Directive 95/46/CE, went further by stating that "natural persons should have control of their own personal data." In other words, it lays a first foundation for the recognition of a right to informational self-determination. The content of this right is specified in the section 3 of the regulation. To already existing rights to be informed, to access, to rectify and to object, the regulation adds the right to restriction of processing (Article 18), to data portability (Article 20) and modifies the right not to be subject to a decision based solely on automated processing (Article 22). The right to erasure, previously restricted to the processing that did not comply with the directive 95/46/CE, has been extended to include cases where:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or processed;

(b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;

(c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for the purposes of direct marketing;

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased to comply with a legal obligation;

(f) the personal data of a child have been collected.

The information obligations imposed on controllers have been further detailed. At the same time, the right to be informed and to object before a disclosure of personal data to third parties has been withdrawn. According to the regulation, if personal data are collected from the data subject (Article 13), the controller must provide the individual with the information on the recipients or categories of recipients of the personal data and, if applicable, on controller's intention to transfer personal data to a third country or international organization. If personal data have not been obtained from the data subject (Article 14), the controller must also provide the information on their source. In case if further data disclosure is envisaged, the controller must inform the data subject "at the latest when the personal data are first disclosed."

An important part of the informational self-determination is the legal means at the disposal of individuals to assert their rights. For this purpose, the regulation provides for a wide range of remedies: a complaint to a supervisory authority (Article 77), a judicial remedy against a supervisory authority (Article 78), a controller or processor (Article 79). Furthermore, it is possible to launch a group action, by mandating a not-for-profit body, active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge a complaint (Article 80).

In France, in the wake of the GDPR, the *Loi pour une République numérique* (Law for a Digital Republic) of 7 October 2016 established the individuals' right to decide and to control the use of the personal data relating to them, under the conditions laid down by the law. That is, the law introduced the right to informational self-determination in France. To the rights mentioned in the GDPR, the law added a right to define directives relating to the conservation, erasure and communication of personal data after death (right to "digital death") and detailed the exercise of children's rights in the health care sector.

To summarise, the European approach seems to combine two visions of data protection: State protection, through controls carried out by national data protection authorities, enhanced by self-protection of individuals through an arsenal of rights. Such a range of rights composing the emerging right to informational self-determination raises the question of how these rights can be exercised in practice.

PART II – PITFALLS IN THE EXERCISE OF THE RIGHT TO INFORMATIONAL SELF-DETERMINATION

According to Article 12 of the GDPR, the controller facilitates the exercise of data subject rights under Articles 15 to 22: to access, to rectification, to erasure, to restriction of processing, to data portability, to object to processing, and not to be subject to a decision based solely on automated processing, including profiling. Furthermore, data subjects exercise their rights free of charge, except for manifestly unfounded or excessive requests. The European legislator therefore expects controllers to provide appropriate and easily accessible technical means, to enable data subjects to exercise their rights. The controller's refusal to take action on the request of the data subject opens the possibility to lodge a complaint with a supervisory authority and to seek a judicial remedy.

However, the application of these provisions raises several questions. First, the Regulation seems to conceive self-determination of individuals within a framework of a bilateral relation "data subject – controller", while data processing has been carried out in a network "data subject – plethora of controllers", which can be called a "networked processing". Furthermore, the majority of controllers remain unknown to the data subject, despite the controllers' obligation, after obtaining the personal data from another source than the data subject, to inform the latter about the processing of his or her data ant their source (Article 14). Even if this obligation was first introduced by the Directive 95/46/CE, long before the GDPR, it remains rather theoretical.

The functioning of the online advertising ecosystem provides a good illustration of this situation. Websites that generate revenue for displaying online advertising can use advertising technology (adtech) tools, analyzing and managing information, notably personal data, for online campaigns[15]. Typically, they would use cookies, tracking pixels, fingerprinting, etc. to collect information about users, their device and their visit of the website. The collected information represents a "bid request". Through the mechanism of real-time bidding advertisers compete for advertising spaces on the website, placing their ads by automated means. "This open auction process involves multiple

[15] UK Information Commissioner's Office. Update report into adtech and real time bidding. 20 June 2019. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

organisations processing personal data of website users[16]. Millions of bid requests are processed every second utilising automation, which involves the leveraging of multiple data sources into user profiles shared throughout the ecosystem."[17] In this fashion, following a single request, personal data can be processed by hundreds of participants. Most of them remain unknown to the user, while the participants invoke impossibility or a disproportionate effort needed to inform the users under Article 14. Such an "invisible processing"[18] makes the exercise of self-determination by individuals technically unfeasible.

Another important topic concerning self-determination is how to verify that controllers apply one's choices as regards processing of personal data. Article 15 provides only for access to "raw" data while inferred data (for example, individual profiles) can contain other data related to the individual, the processing of which has been realised without the data subject's consent or even awareness. Going back to the example of online advertising, a bid request may include various data, notably user's ID, location, search queries, site behaviour, and audience segmentation, i.e. specific facts, interests and other user's attributes.[19] These data are used to create user profiles that can be subsequently "enriched" by data originating from other sources, collected for other purposes or through "data matching". Controllers normally invoke their legitimate interests to provide a legal base for such processing without information and consent of users. At the same time, most users are not aware of this situation and even if they were, they would not be able to fully exercise their right to access, due to the nature of inferred data that do not originate directly from the user but result from data transfers and their analysis. In this light, the effectiveness of Article 15 provisions seems to be in question, since they cannot ensure a regular and substantial individuals' control over processing of their personal data.

The third topic is how to prove the infringement before the judge or the data protection authority. That is possible if the infringement is visible and can be observed directly. The question is how to proceed with invisible breaches or abuse. In fact, it is common for data processing in online advertising networks to handle special categories of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, concerning health or a natural person's sex life or sexual

[16] The report mentions a European association for advertising ecosystem that consists of over 5500 members.

[17] Update report into adtech and real time bidding, *supra*, p.11.

[18] Ibid, p. 22.

[19] Ibid, p. 12-13.

orientation. For instance, bid requests may include fields relating to politics, religion, ethnic&identity groups, mental health, infectious diseases, substance abuse, etc.[20] This information is used for better audience targeting and to avoid serving ads to inappropriate websites. However, under Article 9 processing of such personal data is prohibited, except when certain conditions are met, notably if the data subject has given explicit consent to it. Once again, controllers rely in this case on their legitimate interests as a lawful basis for processing. The UK Information Commissioner's Office (ICO) report proved the controllers' assumption to be wrong by stating that "Organisations can still consider legitimate interests as an Article 6 lawful basis for processing special category data, but they also need an Article 9 condition. […] Market participants must therefore modify existing consent mechanisms to collect explicit consent, or they should not process this data at all."[21] Nevertheless, even if the online advertising ecosystem received from the ICO the official interpretation of GDPR's provisions, there is no guarantee that it will be followed by all the participants (in particular, by those that are not in EU jurisdiction) or by other economic sectors. An investigation carried out by a national DPA might be the solution in such cases. According to Article 58, the DPA can obtain, from the controller and the processor/s, access to all personal data and to all information necessary for the performance of its tasks. On the other hand, such an investigation might be long and costly. At the same time, data subjects do not have access to invisible abuses of their personal data and therefore remain with no possibility to lodge a complaint.

It may be argued that the question of access to inferred data, including special categories of personal data, can be addressed by the legislator. Thus, the UK Parliament recommends that inferred data should be as protected under the law as personal data, including "models used to make inferences about an individual."[22] Furthermore, the 2018 California Consumer Privacy Act provides for the access to inferred data, being included in the definition of personal data (or, as laid down in the bill, "personal information").[23] It has to be taken into account however that such a measure could undermine the

[20] Ibid, p.13.

[21] Ibid, p. 16.

[22] House of Commons. Digital, Culture, Media and Sport Committee. Disinformation and 'fake news': Final Report. para.48. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm.

[23] Assembly Bill No. 375. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. "(o) (1) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked,

viability of the existing business model of "surveillance capitalism" that financially underpins an entire economic sector. The application of CCPA from 2020 might have far-reaching effects in this respect. In any case, the collision between the centralized logic of the GDPR and the "networked" processing would not be easy to address within the existing legal framework.

Further examples of pitfalls could be cited. To address these issues, in addition to developing the legal framework, a considerable change in approach might be necessary: starting with information and education of individuals on their rights and their efficient exercise and ending with self-determination tools built in the code, in other words, technical tools available to any individual to exercise his or her rights. If code is law, then law has to become a code, to ensure its own application.[24]

PART III – APPROACHES TO IMPLEMENT THE INDIVIDUAL'S SELF-DETERMINATION

In my Ph.D. thesis[25] I argued that users needed technical means to assert their rights granted by the GDPR. Such technical means could be integrated by default in the technical infrastructure: on the one hand, to monitor references relating to the individual (personal reputation) as well as to send erasure requests to controllers; on the other hand, to protect one's private life by defining its perimeter regarding collection, use, recording and erasure of personal data by controllers/processors and furthermore requesting its respect by them, through the application settings and machine to machine communication. Without appropriate technical means the right to informational self-determination will remain theoretical.

Indeed, there are already existing solutions going in this direction, for example, Do Not Track (DNT). However, there are no legal or technical requirements for the DNT use. In the vast majority of cases,

directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following: […] (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

[24] LESSIG, L. (2006). *Code : Version 2.0.* New York: Basic Books. p. 211.

[25] SHULGA-MORSKAYA, T. (2017). *Démocratie électronique, une notion en construction*. HOURQUEBIE, F. (dir.). Université de Bordeaux.

it is not taken into account by Web sites. Furthermore, users cannot choose trusted sites or acceptable types of tracking. It appears that a more sophisticated privacy-control mechanism is needed while there should be legal and economic incentives for industry to implement it. To be viable, the solution should therefore combine technical, legal, and economic aspects.

Tim Berners-Lee has been working on a solution of that kind. With colleagues from the Massachusetts Institute of Technology he created Solid[26], a set of conventions and tools for building decentralised social applications. Instead of providing their personal data to each website they use, users would be able to keep them on their own "personal online data store" (POD), a repository with all the personal information they want to share, on a Solid server, on their own site or hosted with a provider. To use an individual application, they would then give permission to read and write to their POD. If they want to quite an application, they could revoke the permission to access their data. In this fashion, the personal data remain at all times on the POD, not on the application's server, regardless of user's activity in the application.

Solid is based on Linked Data principle: every piece of data gets its own HTTP URL on the Web. These URLs are then used to link the data, and those links are standardized, so that different users and apps can reuse the same data at the same time.[27] According to Solid's authors, users' privacy is managed using the Web access control list specification: a decentralized system, which enables users and groups access to resources. Users are identified by WebIDs based on URI - a uniform resource identifier - expressed by a unique string of characters. User groups are identified by the URI of a class of users. As a result, a person hosted by any site can be a member of a group hosted by any other site. External users do not have to be hosted on the site to have access to information, their access relies only on the permission received from the "owner" of the information they want to access. Apart from a certain fragility of the solution to store all the personal data on a POD, decentralised peer-to-peer networking and a possibility to have as many pods as one likes reduce the risk of privacy violation.

It is interesting to mention that Solid creators claim enabling users to have a "true ownership" on their data, although there seem to be no built-in mechanisms for value estimation and receiving benefits

[26] Solid. https://solid.mit.edu/.

[27] Ibid.

from applications for their use of data. On the other hand, Tim Berners-Lee wrote that Solid was guided by the principle of "personal empowerment through data",[28] which would be close to the right of informational self-determination. In this fashion, Solid would implement this right at the technical level. However, the economic aspect of the problem remains unaddressed. In fact, Solid aims to create and expand its own technical infrastructure: Solid PODs hosted on Solid enabled Web servers and applications created especially for Solid using its API.[29] The question is how to attract developers who would create these applications for Solid. At the moment, business models on this market are based on placing advertisements or collection of users' personal data or on both. If data collection is excluded on the platform, would advertisers be interested in non-tailored ads? If none of these models is envisaged, would users be eager to pay for using Solid or to buy Solid applications? It is possible that money was never the motivation for Solid creators and they may expect other developers to follow their way, in order to operate a revolution on the market and to circumvent government and private surveillance. It should be kept in mind, however, that the Internet sector has grown so fast over last decades, notably because it offers unprecedented opportunities for businesses. The economic aspect should not be underestimated.

Another approach to self-determination is proposed by Self-Sovereign Identity (SSI) concept, "bringing the individual to the centre of her data ecosystem and giving her control over the uses of her personal data."[30] If for this purpose Solid focuses on the protected data storage, SSI aims to create a permanent identity for an individual or an entity, based on the distributed ledger technology (DLT), notably blockchain. The SSI identity system includes a digital wallet with collected credentials that can be used to authenticate their owner. Only identity owners would be able to access their full identity and to control what parts of their identity can be shown to others, under revocable permissions. Using self-sovereign identities, individuals and entities would be able to verify information about each other, without having to address to a trusted third party. Users' privacy is managed through decentralization

[28] BERNERS-LEE, T. One small step for the Web… *Inrupt*. 23 October, 2018. https://inrupt.com/blog/one-small-step-for-the-web

[29] Application processing interface, a communication protocol allowing third parties to create applications that use data or services of the given IT system.

[30] WAGNER, K. ET AL. (2018). Self-sovereign Identity. A position paper on blockchain enabled identity and the road ahead. German Blockchain Association. https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf p.12.

and encryption, notably through cryptographic techniques known as "zero-knowledge proofs". It is a method by which one party (A) can prove to another party (B) that something is true, without revealing any information.[31] For example, A can prove to B that A is over 18 without revealing the birth date. The SSI also allows users to "make claims, which could include personally identifying information or facts about personal capability or group membership."[32] Other users may also make claims about a user, so that the user does not control all the claims about him or her. At the same time, the right to erasure (Article 17 GDPR) has to be respected and claims have to be modified or removed as appropriate over time. To exercise full control over the data, "a user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers."[33]

The SSI concept has been largely implemented. The Swiss canton of Zug began providing SSI-based IDs, based on the Ethereum blockchain, for residents to access public services. After signing up for UPort ID App, users are required to visit the city office for in-person verification. The city clerk then issues their Zug ID, signed by the city's identity, that they can use to get access to several services.[34] In 2017 the U.S. State of Illinois launched a pilot project, creating a blockchain-based birth registration system.[35] Among non-governmental projects, Bitnation, the world's first Decentralised Borderless Voluntary Nation (DBVN) implementing the blockchain ID and Public Notary, can be mentioned.[36] Another example, a personal cloud Respect Network, aims to connect people and businesses over direct, personal channels, to share personal data (for example, medical records) under the individual's control.[37] Furthermore, the World Wide Web Consortium (W3C) has created a new Working Group

[31] SCHOR, L. (2018). On Zero-Knowledge Proofs in Blockchain. *Medium*. https://medium.com/@schor/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1.

[32] ALLEN, C. (2016). The Path to Self-Sovereign Identity. *Coindesk*. https://www.coindesk.com/path-self-sovereign-identity.

[33] Ibid.

[34] Zug Digital ID Case Study: Government Issued Blockchain Identity. *Consensys*. https://consensys.net/enterprise-ethereum/use-cases/government-and-the-public-sector/zug/.

[35] YOUNG, A., WINOWATAN, M, & S. VERHULST. (2018). Case Study: Registering Births on the Blockchain in Illinois. GovLab. https://blockchan.ge/blockchange-birth-registration.pdf.

[36] Bitnation. Governance 2.0. https://tse.bitnation.co/.

[37] Respect Network. https://respectnetwork.wordpress.com.

tasked with standardizing the cornerstone of SSI - decentralized identifiers. In the long run, this might transform the Internet in an interoperable ecosystem of connected entities.[38]

It seems that the future of SSI looks bright. Not without downsides, however, that might include a system of multiple platforms with multiple identities for each person, making it difficult and time-consuming to manage personal data and permissions to access them across platforms. Another difficult issue is again the economic one. Distributed ledgers and blockchains include a utility token system. With tokens, users have been rewarded for their actions or services on the blockchain. They can be used for getting access to certain application features, for exchanging for other tokens or real-world money. Thus, some SSI-based applications allow users to gain revenues by selling their personal data to third parties.[39] These applications can be reclassified from self-determination solutions to data "ownership" ones. Other developers have been reflecting on "new business models [based on DLT and using "zero-knowledge proof" method] where users and app creators can earn currency by sharing some of the data without disclosing anything that is personally identifiable."[40] At the same time, tokens open the way to new business models, related neither to data collection, nor to advertising. For example, businesses on the Respect Network "pay *relationship fees*, which are based on the overall value of a customer relationship facilitated by the network",[41] including value of the customer profile and other data that a customer shares over a self-controlled personal channel, customer acquisition and retention value of the channel, etc. Another approach to creation of value is implemented in the Bitnation's business model. It is based on transaction fees related to contract creation and execution within the system. Tokens are also used to calculate user's reputation, to provide incentives for contract compliance, dispute resolution, and, in the long term, "for building and monetizing cooperative behaviour amongst participants."[42] Accumulated reputation is then rewarded with tradable arbitration

[38] WAGNER, K. ET AL. (2018). Self-sovereign Identity, *supra*. p. 9.

[39] See, e.g., Self Sovereign Identity & Decentralized Identity: Control Your Data. *DragonChain*. https://dragonchain.com/blog/decentralized-identity-self-sovereign-identity-explained.

[40] DUJMOVIC, J. Opinion: The good and the bad of Tim Berners-Lee's new project on data privacy. 15 October 2018. https://www.marketwatch.com/story/the-good-and-the-bad-of-tim-berners-lees-new-project-on-data-privacy-2018-10-12.

[41] Respect Network. Business model. https://respectnetwork.wordpress.com/business-model/.

[42] TARKOWSKI TEMPELHOF, S. ET AL. (2017). Pangea Jurisdiction and Pangea Arbitration Token (PAT). The Internet of Sovereignty. https://github.com/Bit-Nation/Pangea-Docs/raw/master/BITNATION%20Pangea%20Whitepaper%202018.pdf. p. 35.

tokens that can be used to pay for governance services on the platform.[43] Meanwhile, the German Blockchain Association expressed reservations concerning the "tokenization" of the SSI-based applications: "The universal solutions for identity should provide a balanced scheme of incentives between all actors within the addressed ecosystem, without giving the initial issuer a power monopoly in the system."[44]

Lastly, and most importantly, the GDPR-compatibility of these solutions raises concerns. The immutability of blockchain, which means that once a transaction is written on a blockchain, it is burdensome to delete it, becomes problematic when facing the need to implement self-determination rights, notably the right to rectification or to erasure. It is possible to make the data inaccessible by using for example zero-knowledge proofs, but it is not clear whether such operations will be considered as compliant with the notion of "erasure" in the GDPR. It is not clear either if the largely debated idea to store transactional data off-blockchain (thus allowing easier rectification and erasure) and to link them to the blockchain through a hash[45] could meet the data protection requirements.[46] Indeed, hashes as well as public keys that cannot be erased from the blockchain are likely to be qualified as personal data, so this would not solve the problem. As well, the continued data processing and the replication of data on numerous computers within the system conflict with the principles of data minimization and purpose limitation. Furthermore, in such disintermediated systems the question of responsibility for data processing and, subsequently, of liability for privacy breaches arises. In the blockchains where a single actor or a group determine the means and, mostly, the purposes of the processing but anyone can register transactions (private and permissionless blockchain), individual companies using such an infrastructure for their own purposes might also qualify as joint controllers,[47] in line with the European

[43] Ibid.

[44] WAGNER, K. ET AL. (2018). Self-sovereign Identity, *supra*. p. 46.

[45] Cryptographic hash is a mathematical function that transforms an input value into an output value of fixed length, with no possibility to deduce the hash input from the hash output.

[46] FINCK, M. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. p.32.

[47] Ibid, p. 45.

Court of Justice's judgment in the *Wirtschaftsakademie Schleswig Holstein* case.[48] The determination of the controller in blockchains where anyone can participate and register transactions (public and permissionless blockchains) becomes even more complicated and should be carried out on a case-by-case basis. It is worth mentioning that, in some cases, natural persons, users of such blockchains, may be considered as data controllers.[49] In other words, their right to informational self-determination would be fully achieved. On the other hand, without a full understanding of data processing technical and legal implications as well as technical means to apply their choices, natural persons may not make full use of their rights.

More generally, such solutions have to be compliant not only with sector-specific regulations (when blockchains process, for example, health data or financial transactions) but also with diverse legal frameworks, in case of international SSI-based applications. These considerations should be taken into account at the application design stage, with a systematic evaluation of legal, technical, and economic aspects.

PART IV – CONCLUSIONS

The GDPR, conceived to reduce the risks of a centralized data processing, is difficult to apply to a networked or decentralized data processing, which represents, however, a reality to be dealt with in order to implement the nascent right to informational self-determination. The paper showed that, at the moment, the full exercise of the right to informational self-determination in the context of networked data processing would not be possible. Furthermore, it is not clear how the GDPR will be interpreted when applied to developing DLT technologies that constitute the technical foundation for emerging informational self-determination solutions. It appears that a further multidisciplinary research, federating the efforts of legal, IT and economic communities, is needed to create privacy-ensuring

[48] Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig Holstein,* C-210/16, ECLI:EU:C:2018:388. http://curia.europa.eu/juris/liste.jsf?num=C-210/16.

[49] FINCK, M. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?, p. 50.

solutions, based on individuals' self-determination. Such solutions may be conceived in different ways and their use may increase legal certainty not only for users but also for companies, through the transfer of responsibility to define and protect individual privacy to individuals themselves. The companies would have to ensure correct functioning of the privacy-control mechanism and the security of collected data, which seem to be easier technical tasks.

More generally, the development of informational self-determination systems revives the question of the legal nature of personal data: if they are a part of identity, insusceptible to alienation, or a disposable property. A reflection on this subject should be closely linked to the issue of the meaning of privacy. In today's interconnected communities, individual privacy depends on other community members' perception and implementation of privacy boundaries. When centralized data silos apply a loose interpretation of privacy norms, they might face legal consequences. When other members of the community apply such interpretation, this might lead to lower privacy standards for all.[50] Such "networked privacy"[51] in decentralized communities based on informational self-determination should require reinforced information and education policies.

[50] See, e.g., SELINGER, E. (2019). Why You Can't Really Consent to Facebook's Facial Recognition. *Medium*. https://onezero.medium.com/why-you-cant-really-consent-to-facebook-s-facial-recognition-6bb94ea1dc8f. "Facebook's facial recognition policy may be legal but it fails the consentability standard by obscuring risk and corroding collective autonomy. […] It's not just that law enforcement can get information from tech companies. It's that the more the private sector engages in facial surveillance, the harder it becomes to tell law enforcement that their access should be meaningfully restricted."

[51] BOYD, D. (2011). Networked Privacy. www.danah.org/papers/talks/2011/PDF2011.html.