LEX ELECTRONICA

2021

VOLUME 26 | NUMÉRO 1

DATA OWNERSHIP *VERSUS* DATA SHARING: AND WHAT ABOUT PRIVACY?

Yann Padova[1]

38

DATA OWNERSHIP *VERSUS* DATA SHARING: AND WHAT ABOUT PRIVACY?
Yann Padova

1 Avocat, Partner chez Baker MccKenzie Paris en charge de la pratique « données personnelles ». Ancien Secrétaire général de la CNIL (Commission nationale de l'informatique et des libertés) en France, ancien Administrateur (haut fonctionnaire) à la Commission des lois de l'Assemblée nationale, spécialisé dans le droit du numérique et le droit pénal

TABLE DES MATIÈRES

SUMMARY :

- Several initiatives, both in the EU and in the US, have recently claimed for the introduction of property rights over personal data. Data propertisation is conceived by its supporters as the legal instrument for individuals to take control of their own data, consequently equating the right of ownership to data and controlling how they are used.

- Such revival of data propertisation claims mostly flows from the entry into force of the GDPR notably through the introduction of the right to data portability which is seen as a "step" towards propertisation of personal data.

- On the other side of the spectrum, the call for propertisation of data is also supported by companies in order to obtain the legal recognition of their informational and intangible assets and, as a result, to secure the legal basis for the commercial use of personal data, and in particular to ensure control and financial value for selling it.

- Simultaneously, equally numerous arguments are developing to encourage, or even require, companies operating in specific sectors such as environment, transportation, employment and housing, to share their data. However, the legal ground for such mandatory sharing proves itself to be legally challenging to establish.

- Data in general, and personal data in particular, seem to be truly torn between contradictory injunctions and these paradoxical demands stem from different, even contradictory, public policy objectives.

- However, from a European civil law perspective which will be the focus in this article, data propertisation falls short of increasing the control by individuals over how their data are used and of improving the collective well-being ensured by a high level of data protection which may qualify as a "public good". An individual's ownership of data does not lead to more control over their use and a better level of protection, quite to the contrary. Conversely, more control by individuals over the use of their data does not require the introduction of a right of ownership to such data.

- As per mandatory data sharing claims, they focus on the issue of access to data and underestimate the importance of the systemic and

legal conditions that are conducive to using them in order to foster innovation.

Keywords: Data Governance Act /data in the general interest / data ownership / data sharing for innovation / individual control over personal data / propertisation of personal data.

RÉSUMÉ :

- Plusieurs initiatives, tant dans l'Union européenne qu'aux États-Unis, ont récemment réclamé l'introduction de droits de propriété aux données personnelles. La propriété des données est conçue par ses partisans comme l'instrument juridique permettant aux individus de prendre le contrôle de leurs propres données, assimilant ainsi le droit de propriété aux données et le contrôle de leur utilisation.

- Ce renouveau des revendications en matière de propriété des données découle principalement de l'entrée en vigueur du RGPD, notamment par l'introduction du droit à la portabilité des données, qui est considéré comme un « premier pas" vers la propriété des données personnelles.

- De l'autre côté du spectre, l'appel à la propriété des données est également soutenu par les entreprises afin d'obtenir la reconnaissance juridique de leurs actifs informationnels et immatériels et, par conséquent, de sécuriser la base juridique de l'utilisation commerciale des données personnelles, et en particulier de garantir le contrôle et la valeur financière de leur vente. Simultanément, des arguments tout aussi nombreux se développent pour encourager, voire obliger, les entreprises opérant dans des secteurs spécifiques tels que l'environnement, les transports, l'emploi et le logement, à partager leurs données. Toutefois, le fondement juridique de ce partage obligatoire s'avère difficile à établir.

- Les données en général, et les données personnelles en particulier, semblent véritablement tiraillées entre des injonctions contradictoires et ces demandes paradoxales découlent d'objectifs de politiques publiques différents, voire contradictoires.

- Cependant, dans la perspective du droit civil européen qui sera celle adoptée par cet article, la propriété des données ne permet pas d'accroître le contrôle des individus sur l'utilisation de leurs données et d'améliorer le bien-être collectif assuré par un niveau élevé de protection des données qui peut être qualifié de "bien public". La propriété des données par un individu ne conduit pas à un plus grand contrôle de leur utilisation et à un meilleur niveau de protection, bien au contraire. Inversement, un plus grand contrôle par les individus de l'utilisation de leurs données ne nécessite pas l'introduction d'un droit de propriété sur ces données.

- Quant aux revendications de partage obligatoire des données, elles se concentrent sur la question de l'accès aux données et sous-estiment l'importance des conditions systémiques et juridiques propices à leur utilisation pour favoriser l'innovation.

Loi sur la gouvernance des données /données d'intérêt général / propriété des données / partage des données pour l'innovation / contrôle individuel des données personnelles / appropriation des données personnelles.

In March 2019, U.S. Senator Kennedy introduced a bill, the Own Your Own Data Act, to introduce a right of ownership for individuals to their data (U.S. Sen. Kennedy, Act, S806, 2019). On the other side of the Atlantic, but this time in January 2018, the French liberal think-tank Génération Libre published a report along the same lines (*Génération libre*, 2018), to work "*towards the propertisation of personal data*" and claiming for the application to personal data of the traditional civil law regime of property. In 2017, the European Commission itself published a study on the, "*emerging issues on data ownership, (re)usability and access to data, and liability*", indicating its interest in this issue (Deloitte, 2017).

This recent profusion of initiatives reopens a debate the concepts of which are quite old. Indeed, this issue has existed in the scientific community and among data protection practitioners for nearly 20 years. In fact, its intellectual origins can be traced to American academic writings, such as the work of Professors Pamela Samuelson (Samuelson, 1999, p. 1125*)* in 1999, and Paul Schwartz in 2003 (Schwartz, 2003, p.2056).

So why is this debate now experiencing such a revival?

Several factors contribute to this. First of all, the entry into force of the General Data Protection Regulation ("GDPR") (EU Regulation 2016/679 (GDRP))[2], which may be perceived as a step (Génération Libre, 2018, p. 77) in this direction, notably through the introduction of a new right for individuals – the right to data portability[3]. And regulators themselves, such as the ICO[4], refer to "*data ownership*".

Secondly, other analyses, are based on the existence of an unequal exchange between companies collecting data and data subjects whose "work" for these companies deserves compensation (Lanier, p. 38, 2018). From this, these analyses deduce the need for data subjects to receive fair financial compensation, which the recognition of a right of ownership to

2 Apr. 2016, entered into force on 25 May 2018.

3 The right to data portability provided in Article 20 of the GDPR states that data subjects "shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided", insofar as such data have been collected based on the individual's consent or within the framework of a contract's performance.

4 Information Commissioner's Office (ICO), "Your data matters", "But your data is your data. It belongs to you so it's important your data is used only in ways you would reasonably expect, and that it stays safe." (author's emphasis), https://ico.org.uk/your-data-matters/

their data is supposed to facilitate. These arguments, based on an "economic" analysis of the data collection and processing circuit presupposes the existence of high data value that is purportedly hidden. And, the introduction of a right of ownership would help uncover this value.

However, the experiments carried out in the field of data monetization appear to be inconclusive (Harrison, 2018)[5], with the price received rarely reaching more than 10 dollars. The corollary to overestimating raw data's value is underestimating the cost to companies of the investments[6] required to analyse such data and to create value from it. This is because data's value comes from analysing them, not from the raw data taken in isolation. The fact that many services accessible online are free of charge and financed by advertising appears to have had the effect of convincing people that these services have no cost for the companies that offer them and that they are now a "given" for users, much like a sort of free digital universal public service.

In essence, there are different types of analyses of the arguments of proponents of data propertisation, which are not necessarily consistent with each other: data propertisation is conceived by some as the legal instrument for individuals to take control of their own data, consequently equating the right of ownership to data and controlling how they are used. Yet, the call for propertisation may also be supported with a view to providing for the necessary legal recognition of companies' informational and intangible assets and in order to retribute and stimulate innovation (Kroes, 2013). The aim is (i) to secure the legal basis for the commercial use of personal data, and in particular, to ensure control and financial value for selling it and (ii) to stimulate data driven innovation. In this scenario, the beneficiary of data propertisation is no longer the data subject, but instead, the company.

Simultaneously with these calls for applying the ownership regime to data (although the beneficiaries may be different), equally numerous arguments are developing to encourage, or even require, companies, and in particular those identified as being dominant in the digital economy, to share their data (Mayer-Schönberger & Ramge, 2018, p.48). This call for

5 . Several companies are trying to build their business model on personal data monetization directly with the user (money in exchange of personal data) such as Datacoup in the UK or Tadata in France which specifically targets teenagers.

6 As an illustration, Microsoft's research and development expenditures in 2018 reached 13% of its turnover, 19% for Facebook and 15.6% for Google.

sharing, which historically began with the development of Open Data policies reserved for public data, is now being gradually extended to private companies without a public service mission. And the concept of "data in the general interest" is the legal instrument for this extension. Initially created by the French Parliament[7], this concept also appears to be convincing European institutions since the European Commission firstly created a group of high-level experts on this subject whose report was made public in 2020 (European Commission, 2020) and, secondly, now refers to *"data altruism"* in its recent draft regulation on European Data Governance Act ("DGA") which encompasses both personal and non-personal data (European Data Governance, 2020)[8].

This call for mandatory sharing presupposes that data are rare, concentrated, and not abundant or easily accessible[9]. However, there are contradictory analyses and information in this area, with some suggesting a "*flood*" of data (Institut Montaigne, p.15, date?)[10], and others a scarcity and concentration requiring the introduction of a data sharing obligation. The European Commission communication on a European strategy (European Commission, 2020, p.4,)[11] for data, which echoes the 2018 report on AI of the mathematician and French MP Cédric Villani, is part of this trend focusing on data concentration (Villani, p.14, 2018)[12].

In this communication, the European Commission first of all highlights the volume of available data, and, therefore, their relative abundance, but it then stresses the need to increase use of data in order to have "*better decisions (European strategy for data,* p. 5*).*" And the Commission proposes several measures to encourage companies to share their data more amongst one another and with public bodies. With regard to what is referred to as "B2G" sharing, the Commission appears firstly to favour incentives, while clearly indicating that, secondly, requirements for

7 Introduced by Art. 17 of Act No. 2016-1321 of 7 Oct. 2016, referred to as the Act "for a digital Republic".

8 See the Proposal for a Regulation on European Data Governance (Data Governance Act), COM (2020) 767 final, Art. 2 § 10 which defines "data altruism" as meaning "the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services".

9 *See* the joint report of the French and German competition authorities; "*Data and competition Law",* 2016, p.13

10 *See* the report from think tank ": "The Internet of things purportedly contributes to doubling the size of the digital universe every 2 years, which could represent 44,000 billion gigaoctets in 2020, or 10 times more than in 2013," p. 15.

11 "Currently, a small number of Big Tech firms hold a large part of the world's data. This could reduce the incentives for data-driven businesses to emerge, grow and innovate in the EU today, but numerous opportunities lie ahead",

12 "*Today, data benefit mainly a handful of very large players. It is only with greater access and better circulation of these data, to benefit not only public authorities, but also smaller economic players and public research, that it will be possible to restore the balance of power*."

companies to share their data could be introduced, "*where specific circumstances so dictate, access to data should be made compulsory, where appropriate under fair, transparent, reasonable, proportionate and/or non-discriminatory conditions (European strategy for data,* p. 13)." But it is worth noting that the DGA does not contain such compulsory data sharing requirements.

Data, therefore, seems to be truly torn between contradictory injunctions, some of which advocate ownership for individuals or legal entities, which involves, as does any right of ownership under civil law regime, that of not sharing and excluding beneficiaries. Other demands favour an obligation, solely for companies, to share their data due to the expected benefits for innovation and competition, at the risk of infringing on the right of ownership.

These paradoxical demands stem from different, even contradictory, public policies objectives. And to determine what is the *"regulatory end goal"* is not easy (Worthington, p.10, 2018). Does it aim at strengthening individuals' control by recognizing a right of ownership to their data? Is the purpose of propertisation to protect individuals' creation by granting them a right of ownership to their data? In these scenarios, the logic that undergirds the introduction of this right is the strengthening of individuals' control over the use of data, or even possibly excluding certain beneficiaries.

Or, conversely, is requiring companies to share their data being considered to facilitate innovation and break up the monopolies of non-European companies by following a logic of inclusion, as opposed to a logic of exclusion, as previously discussed? However, is this obligation based on the observation of the scarcity of data or the opposite, under-use of data that is nevertheless abundant? The objectives then pursued are more in line with industrial policy but potentially undermine companies' right of ownership and right to trade secrets, a concept recently introduced into European law[13].

Faced with this complex situation, the objective of this article is threefold. Firstly (I), it will outline the reasons that are leading to the current revival of the debate on data ownership and discuss the soundness of

13 EU Directive 2016/943 of 8 Jun. 2016, implemented under French law with Act No. 2018-670 of 30 Jul. 2018 on trade secrets.

arguments in favour of data propertisation mostly from a European data protection perspective. Secondly (II), it will examine the bases of the growing number of calls for data sharing, with particular emphasis on the legal nature of the new concept of *"data in the general interest"*. Thirdly, (III), it will consider whether the application of civil ordinary law on ownership of property to personal data would be beneficial to the rights of the data subject and their level of data protection.

I. PROPERTISATION OF DATA, A NEW MISCONCEPTION?

1A – PROPERTISATION OF DATA, AN OLD DEBATE REVIVED BY THE GDPR

Legal and economic scholarship and theory on data control and ownership were initially debated in the United States in the late 90s (Hagel III & Rayport, 1997). They contrast with the European approach, first enshrined in the Council of Europe Convention of 28 January 1981, then in Directive 95/46/EC of 24 October 1995 on the protection of personal data. Indeed, the protection of individuals with regard to the processing of their personal data is being built in Europe through what is referred to as a personalist approach, which recognizes that all human beings have fundamental rights and freedoms, including data protection (Charter of Fundamental Rights of the European Union, Art. 8)[14]. As a result, no privacy or data protection laws expressly define which entity *owns* personal data (Ritter & Mayer, p. 261, 2017) which triggers challenging questions such as "who" shall own the data or when does ownership attach to data?

Carl Shaprio and Hal Varian consider the personalist approach too rigid, or even economically inefficient (Shaprio & Varian, 1997). According to the classical theory of the right of ownership, originally developed in relation to land (John Locke, 1690, par.27)[15], the effect and benefit of this right is to encourage the maintenance of property and the creation of value by guaranteeing the owner fair compensation for his efforts. Given the

14 " *Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."*

15 *"Though the earth, and all inferior creatures, be common to all men, yet every man has a property in his own person: this no body has any right to but himself. The labour of his body, and the work of his hands, we may say, are properly his. Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his labour with, and joined to it something that is his own, and thereby makes it his property. It being by him removed from the common state nature hath placed it in, it hath by this labour something annexed to it, that excludes the common right of other men."*

influence of this school of thought in the Anglo-Saxon world, quite logically an approach based on the recognition of a right of ownership to personal data has been gradually constructed through the prism of an economic analysis of law. The propertisation of personal data is then seen as a legal tool both to correct market failures and to protect the interests of individuals.

Market failures in the area of data protection are the result of the gap between, on the one hand, the significant income data can bring to the companies which collect them and, on the other hand, the absence of a real cost or high risk for them when they misuse such data. In other words, the market's imperfections lie in the fact that income is internalized by companies, while losses and potential damages[16] are externalized to the detriment of individuals.

In the absence of a corrective mechanism, this situation creates a powerful and systematic incentive for companies to accumulate data. At the end of the 90s, these analyses (Samuelson, 1999, p.1126) particularly highlighted two types of income resulting from the accumulation and use of personal data for the relevant companies: (i) accumulation of data allows companies to better promote their own goods or services while (ii) increasing profits from selling such data to third parties (Swire & Litan, 1998).

Given these imperfections, in 1999, Lawrence Lessig (Lessig, 1999) proposed the creation of a personal data market and recognition of a right of ownership for individuals to their data. Within this framework, individuals could negotiate with the companies that use their data. The purpose of these negotiations would be to determine individually, through a cost-benefit calculation, the extent to which it would be beneficial for individuals to allow their data to be used.

Another benefit of introducing a right of ownership would lie in the income that individuals could derive from the use of their data, which would be subject to financial compensation. This right would thereby contribute to modifying the circuit for creating value on the data market by making it more equitable due to the participation of new actors: data subjects (Laudon, 1996, points 92-100). Thus empowered with negotiation

16 Potential damages such as identity theft, misuse of data, data losses due to cybersecurity breaches, reputational damage, unfair discrimination, civil liability etc.

leverage, each individual could adapt his or her own preferences on the data market. The pricing mechanism and price fluctuation would make it possible to achieve a balance between the offer and demand of solutions adapted to the duly negotiated preferences of each individual.

The second benefit would arise from the fact that the potential compensation based on the right of ownership would have the effect of forcing companies to internalize certain costs from collecting and using personal data. Thus, companies would be incentivized to make different trade-offs that would influence their decisions to invest, or not invest, in purchasing particular data. This constraint would, therefore, maximize social welfare by introducing an incentive to minimize data collection - which would promote privacy protection - due to the increase in the personal data's price. Moreover, companies would be incentivized to develop higher-quality databases in order to avoid unnecessary investments.

As one can see, the idea of a right of ownership for individuals to their data is clearly the result of an analytical approach that applies the conceptual framework of how the market functions to personal data, an intangible object. This idea has gained traction given the entry into force of the GDPR. Indeed, and as Génération Libre points out in its report, the GDPR represents, "*a step in the direction*" of propertisation (Génération Libre, p.77).

1B – THE GDPR, A STEP IN THE DIRECTION OF DATA OWNERSHIP?

When we refer to the traditional civil-law definition of ownership, this means the right "*to enjoy and dispose of things in the most absolute manner* (French Civil Code, Art, 544)" which imply the following legal attributes: *abusus, fructus* and *usus.*

Usus, in other words the right of direct use of property, carries with it the right to possess and use a thing without receiving the fruits from it. Applying usus to personal data is possible, for example, when a person freely decides to sign up on an online e-commerce website and to provide

his or data in exchange for creating an account[17]. However, "*it is difficult to conceive of the usus of another's data in the event of a transfer of ownership: a third party would then acquire the right to use another's data, which may lead to unacceptable situations. If identity data is sold, identity theft could therefore become legal*," as Fabrice Mattatia and Morgane Yaïche point out (Mattatia & Yaïche, 2015, p.2).

As for *fructus*, this is the right to receive the fruits or the income that may be derived from selling the property. This is the intrinsic objective of ownership. Although experiments aimed at monetizing data have had mixed results (Harrisson, 2017) one cannot rule out the principle that *fructus* is applicable to personal data.

As regards *abusus*, which means the right to dispose of the thing possessed as one wishes, including the right to exclude certain individuals from using it, this is the principal characteristic of the right of ownership, if not the *sine qua non* condition of its existence (Merill, 1998, p. 730). As a result the owner of property is free to prohibit access to it by a person, to destroy it or to convey it to a third party by transferring ownership to that person. This new owner then has the same prerogatives as the previous one, and may in turn exercise his *abusus* to the transferred property. Is such reasoning applicable to personal data? Nothing is less certain. Indeed, it seems difficult to transfer to others the right of *abusus* to our personal data and, therefore, to authorize them to delete them, at the risk, for example, of destroying "*our identity* (Mattatia & Yaïche, 2015, p.3)."

However, the rules of data protection envisage a certain number of hypothetical situations where the individuals are effectively able to exercise a right of exclusion on the use of their data. For example, under the GDPR, when processing of the data is based on obtaining the data subject's consent (GDPR, Art. 4)[18], the data subject is theoretically free to refuse his or her consent and may subsequently withdraw such consent at any time. The data subject may, therefore, exclude certain uses of his

17 This situation may be captured by the common law notion of "consideration" as explained by Magali Eben, in *Market Definition and Free Online Services: the Prospect of Personal Data as a Price*, Journal of Law and Policy, 14, p. 240, 2018. Consideration is defined as the reciprocity that makes a contract legally binding, when each party to a contract is both promisor and promisee of something of value, here the personal data. And consideration does not require money per se. Indeed, an American court held that, despite the lack of monetary price in the case of the exchange of personal data for a service, there had been sufficient consideration for a contract to be established. Eben refers to the case *Gotlieb v. Tropicana Hotel & Casino*, 109 F . Supp. 2d, 324, 329, (E.D. Pa. 2000).

18 "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data *relating to him or her*." Other legal grounds are avaiblable for data processing, such as the performance of a contract or the legitimate interest of the data controller pursuant to Article 6 1°, b), f) of the GDPR

or her data. Similarly, the data subject "*shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her* (GDPR, Art.21)" when the processing is legally based on the legitimate interest pursued by the controller or on the carrying out of a public-interest mission. Here again, a right of exclusion therefore appears to exist, but it is not absolute or discretionary as *abusus* requires.

Indeed, in order to object to the processing of his or her data, the data subject must justify doing so on, "*grounds relating to his or her particular situation,*" which is far from the manifestation of an absolute prerogative deriving from a right of ownership. Moreover, the GDPR provides that a company processing the data of a data subject who is exercising his or her right to object must stop the relevant processing, "*unless [it] demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims* (GDPR, Art.21)." Nothing seems more legally remote from *abusus* as this possibility for a company to balance its compelling, legitimate grounds with the data subject's rights and freedoms and to allow its interests to prevail over those of the data subject.

In addition, the introduction by the GDPR of a "*right to be forgotten* (GDPR, Art.17)[19]" is, at first glance, akin to the right of exclusion. Yet, in detail, it departs substantially from it. Indeed, this right is subject to several conditions that provide a framework for its scope. For example, the right to be forgotten will not be implemented by the company which receives the request unless, "*the personal data are no longer necessary in relation to the purposes for which they were collected*", or if the, "*data subject withdraws consent*", and there, "*is no other legal ground for the processing.*"

This last clause is important since it demonstrates that, even in the event the data subject withdraws consent, the company could continue to process his or her data if it has a relevant legal ground. This possibility of "neutralizing" the effects of a withdrawal of consent is an element that is completely contrary, in spirit and legal effects, to the attributes of *abusus*.

19 which provides for the data subject's right "to obtain from the controller the erasure of personal data concerning him or her without undue delay."

As regards the right to data portability (GDPR, Art.20), some, such as Génération Libre, have seen it as the recognition of data subjects' right of ownership to "*their*" data[20].

It is undeniable that the purpose of this possibility for data subjects to recover the data they have provided is to strengthen the data subjects' control over processing. This indicates a form of appropriation of the data and subsequent use of them for the benefit of the data subject. However, this right is neither unconditional nor absolute. Indeed, only data collected on the ground of the data subject's consent or of the performance of the contract fall within the scope of the right to portability[21]. Data collected on the ground of legitimate interest are, therefore, excluded, much as are data which are necessary for safeguarding the data subject's vital interest or those collected within the framework of a public interest mission.

As the GDPR's rapporteur clearly stated before the European Parliament's LIBE Commission, portability is above all a way of increasing competition in an area where natural monopolies based on a network's technical specialities regularly appear (Albrecht, p.4, 2012). This analysis was restated by the Article 29 Working Party, which considered that,

> *"Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers[22]".*

Portability, therefore, has as much an objective of appropriation by data subjects as an objective of increasing competition[23] through the technological neutrality it guarantees.

Working Party 29 further states that,

20 Data portability, "enshrines the control of data by the initial sender and, therefore, the appropriation of such data", Génération Libre (n 2), p. 61.

21 As stated by Purtova, (n 37) p. 24, "Making the right to data portability independent of the grounds of processing works towards establishing the data subject's default entitlements in his/her personal data". But the LIBE Committee decided to narrow down the scope of the right to portability

22 WP Opinion 242 rev.01 of 5 April 2017, p. 3. The Article 29 Working Party brought together all the data protection authorities in the European Union in accordance with Article 29 of Directive 95/46 EC.

23 Viktor Mayer-Schönberger and Thomas Ramge, (n 14), p. 54.

> *"Data portability does not automatically trigger the erasure of the data from the systems of the data controller, and does not affect the original retention period applying to the data which have been transmitted. The data subject can exercise his or her rights as long as the data controller is still processing the data*[24]*"*

Data that have been subject to a portability request may, therefore, remain in the company's database, which, once again, illustrates the gap separating the effects of this right from those of *abusus*.

Thus, the GDPR represents "*a step*" in the direction of data ownership. But, it is a very modest step that "*falls short of ownership*", as stated by Teresa Scassa (Scassa, 2018, p.13).

Indeed, the cornerstone of the GDPR and of European "personalist" regulation remains the data controller with which the data subject may exercise his or her rights. Yet, it is indeed the controller who decided to collect the data. This decision-making power to collect data is, as Génération Libre acknowledges, a, "*key element of the legal regime of data*" *(Génération Libre, p.67).* It is also the controller who determines the purposes and means of the data collection and processing (Ritter & Mayer, p.268, 2017)[25], not the data subject. The data subject has no responsibility in processing his or her data, unlike the owner of property. On the contrary, the data subject has no liability for his or her "*household*" use of personal data (GDPR, Art.2).

A natural person whose data are collected lacks some essential attributes of ownership, and, in particular the ability to negotiate, sell, initiate transactions and find buyers for his or her personal data. If the data subject were the rightful owner of his or her data, then any collection without his or her knowledge would be theft, which is not the relevant applicable legal framework in Europe. The determination of the rightful owner of personal data being such a complex and debated issue, Lothar Determann has even come to the conclusion, based more on a common law analysis, that, "*no one owns the data*" (Determann, 2018).

The situation is different in countries with a Roman civil law tradition. For example, it is interesting to point out here that, in a decision of 20 May

24 WP Opinion 242 rev01, (n 52), p 9.

25 The controller, therefore, exercises narrow control over data, which is one of the criteria for identifying ownership under common law.

2015 (French Supreme Court, 2015), the Criminal Chamber of the French Supreme Court (Cour de cassation) accepted the categorization of data theft to a company's detriment, thereby recognizing that data can be "*another person's thing*" (hence this person's property) and thus be subject to "*fraudulent substraction*", the very legal definition of theft. As the French Supreme Court stated, the data had been fraudulently copied by the perpetrator "*without the consent of their owner*", meaning the victim company, the rightful owner of the data protected by the right to property. However, this recognition of data ownership, mostly to companies' benefit, was at the same time accompanied by numerous requests or calls by the public authorities to share data.

II. DATA IN THE GENERAL INTEREST: AN "OPEN DATA" FOR PRIVATE COMPANIES?

2A – FROM TRANSPARENCY TO DATA SHARING

Initially, the Open Data movement was aimed at protecting users against the threats of an intrusive digital administration, the opaqueness of its decisions and the risks of arbitrariness (AJDA, 2016). To this end, the Act of 17 July 1978 introduced into French law the principle of communicability of administrative documents[26]. However, this right was subject to numerous exceptions and was exercised only after an express request by the data subject.

The next, more recent, stage stems from the digitization of the operations of public administrations and the awareness of the volume and value of the data thus produced, both for users and for society as a whole, thanks to the various innovations and services they are likely to generate. This desire to open up access to public data required the intervention of the European lawmaker, which has gradually extended the material scope of the principle of free re-use of public data. Such extension was carried out in 2019[27] when Directive 2003/98/EC on open data and the re-use of public sector information was amended.

However, the French lawmaker went further, introducing the concept of "*data in the general interest.*" This concept appeared in 2015 when a report on this subject, prepared at the Government's request, was made public

26 The Freedom Information Act in the UK, dated 11 Nov. 2000, has the same purpose.

27 Directive 2019/1024 repealing Directive 2003/58. Data produced by public companies acting as public service operators and present in the water, energy, transport and postal services sectors will henceforth be within the material scope of public data re-use.

(French General Economic Council, the French Council of State and the French General Finance Inspectorate, 2015)[28]. Although "*data in the general interest*" now appears in French Law (Digital Republic, 2016, Art.17), this concept is not legally defined, which "*perplexes* (C. Metayer, p. 104)" some commentators. Its current material scope is determined by sectoral legal provisions which encompass data produced by private companies with public service missions that must be made publicly available[29]. However, the 2015 report[30] proposed to go much further by including, within the legal scope of "*data in the general interest*", data produced by strictly private companies which do not carry a public service mission (French General Economic Council, the French Council of State and the French General Finance Inspectorate, 2015, p.52). The identification of these private companies would be based on a sectoral approach and would, in priority, apply to companies operating in the following sectors: environment, transportation, employment and housing.

The European Commission appears to be gradually moving in this direction. Indeed, in 2018, the Commission stated that it was, "*too early for horizontal legislation on data sharing in business-to-business relations* (Communication of the European Commission, 2018, p.11)." Instead, it advocated for the introduction of contractual mechanisms that encourage companies, "*to engage in data partnerships, i.e. arrangements with other companies designed to make the most out of data by as many commercial players as possible*". But, in its 2020 Data Strategy, the Commission is now considering the introduction of an obligation of horizontal sharing of certain data produced by companies on the one hand and, on the other hand, it recommends the creation of nine common European data spaces targeting strategic sectors of areas in the public interest (European Data Strategy, p.22) which may be subject to a data-sharing obligation.

However, the Commission's position seems rather unstable since the DGA draft does not entail mandatory data sharing provisions. On the contrary, it provides for the creation of *"data sharing services providers"* aiming at

28 Report on data in the general interest, prepared jointly by the French General Economic Council, the French Council of State and the French General Finance Inspectorate, Sept. 2015. This report was part of the preliminary work for the drafting of the Bill for a Digital Republic.

29 Such as concessionaires or managers of energy distribution networks, in accordance with Art. 18 et seq. of the Act.

30 Recommendation No. 11 of the report (n 57): "Open by sector and on a case-by-case basis data held by private persons, provided that such opening is justified on general interest grounds and is based on proportionate means."

building confidence[31] in order to foster voluntary, and not mandatory, data sharing between companies (B2B sharing) and between data subjects and companies (B2C sharing).

Though contemplated by the EU Data Strategy, plans for mandatory data sharing raise serious legal questions, in particular with regard to their compliance with the right to private property, freedom of enterprise and database and personal data protection. However, these legal issues are, surprisingly, not deeply analysed nor discussed both in the Commission's data strategy and in the high-level expert's group report on B2G[32].

2B – WHAT GROUND FOR MANDATORY DATA SHARING?

French case law has already established that companies own the data. Consequently, an obligation to share the data they have produced would represent an infringement of their right of ownership. Under French law, such infringement is legal only if it is based on a clearly established public interest ground. What could the ground be? The 2015 report lists several, including the ground relating to "*economic development*" (French General Economic Council, the French Council of State and the French General Finance Inspectorate, 2015, p.46). However, the general and imprecise nature of this objective, as it stands, is probably not such as to satisfy the requirements of precision and proportionality when involving an infringement of a constitutionally protected right such as property.

Moreover, to justify a general interest objective relating to economic development, it would likely be necessary to prove a failure of private initiatives resulting in significant social and economic harm. French administrative case law is familiar with the criterion of the "*failure of private initiatives*" to justify public intervention (French Council of State, 1930). The European Commission appears to draw inspiration from this legal framework, as the failure of the market is also among the criteria it

31 See in particular articles 9 and 11 of the DGA that entail several provisions with a view to building confidence in these new intermediaries from which an increase in data sharing is expected. For instance, article 11 provides that "the [data sharing] provider may not use the data for which it provides services for other purposes than to put them at the disposal of data users and data sharing services shall be placed in a separate legal entity" and further states that "the provider offering services to data subjects shall act in the data subjects' best interest when facilitating the exercise of their rights, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses"

32 The report from the high-level expert group (n 16) states that "[It] should also ensure that the competitive position of private companies and civil-society organisations, or their value chains, is not undermined and that B2G data sharing does not distort competition" (p. 42) and further mentions that "likelihood of the harm" to the company should be assessed but without providing any criteria or a methodology to conduct such assessment.

takes into account when considering the possibility of introducing a data-sharing obligation (European Commission, 2020, p.13).

However, proof of the existence of a private failure to share data remains to be established. The European Commission's report certainly stresses that, "*there is not enough private sector data available for use by the public sector to improve evidence-driven policy-making and public services*" (European Commission, 2020, p.7). Yet, making this insufficiency a failure is a difficult step to take in the legal reasoning.

European *sui generis* law on databases[33] is also a serious obstacle to the introduction under national law of "*private*" data in the general interest that would require companies to share them. On the one hand, this right protects databases in which companies have made substantial investments and, on the other hand, it does not provide for a derogation on grounds that are close to a general interest related to "*economic development*". Indeed, Article 9 of Directive 96/9 provides for only three derogations to the legal protection of databases[34]. And, as this is an exhaustive list, it represents a major supra-legislative constraint on any national initiative that could infringe on the rights of businesses and the databases they have created.

Presuming that the European or national legislature nevertheless commits itself to creating "private" data in the general interest, a number of operational obstacles would then arise. For example, it would be difficult to imagine the Legislator itself defining with sufficient precision what these data in the general interest produced by companies are. Given the diversity, heterogeneity and volume of the relevant data, the Legislator would have to delegate this task, e.g., to an independent administrative authority. However, in any event, the administrative authority in charge would in turn be confronted with serious difficulties given the asymmetry of information between itself and the relevant companies.

The call for sharing is based on the assumption that the data, being in principle a "non-rival" good, may be shared without hindrance. This

33 Directive 96/9/EC of 11 March 1996 on the legal protection of databases, implemented under French law by Act No. 98-536 of 1 July 1998.

34 The three derogations provided for in Article 9 of Directive 96/9 are related to: 1) the use for private purposes of the content of such database; 2) extraction, for illustrative purposes, for teaching or scientific research; and 3) re-use of the database for public security purposes or the purpose of administrative or judicial procedure. None of these derogations contemplates market failure.

reasoning leads to a debatable equivalence between the non-rivalry of the data and the harmlessness of sharing them. Indeed, the fact that a company can access data without such access depriving others of the data does not mean that such access, if made mandatory by regulations, would have no effect on the economic and financial situation of the company that initially produced them. As we have seen, the objective of strengthening competition is very often at the heart of the call for sharing data. It is therefore undisputed that this sharing has effects on how the market functions and on competition between companies.

Consequently, any creation of a category of private data in the general interest should be preceded by a rigorous analysis of the market and of the impact on the situation of the companies potentially affected by its application. Failing this, many undesirable economic or industrial effects could occur. As the economist Joëlle Farchy expressed it, "*sharing data indiscriminately would ruin the expected gains in competitiveness*[35]."

Lastly, this analysis, which focuses on the issue of access to and sharing of data, underestimates the importance of the systemic and legal conditions that are conducive to using them. For is innovation just a question of access to resources, or does it also – and above all – require a favourable and incentive-based legal framework? In this respect, British regulators have understood the link between regulatory innovation and competitiveness. They organize themselves in order to make innovation an instrument to strengthen companies' competitiveness through the so-called "sandbox" technique[36], thereby demonstrating that the approach based on innovative uses of data is just as, if not more, important than the mere issue of access to data.

III. PROPERTISATION: THE END OF DATA PROTECTION?

Let us assume here for a moment that the proposal to apply the civil ordinary-law (*droit commun*) regime of property ownership to personal data is adopted in Europe. What would be the consequences and limits of doing so? They appear to fall into two categories: on the one hand, economic and practical, and, on the other hand, legal, which "we" are examined successively below.

35 Op-ed published on 3 December 2018 in the newspaper Le Monde, "we must have a data-sharing ecosystem that is sustainable over the long term."

36 The Financial Conduct Authority (FCA) implemented the first "sandbox". The ICO in turn committed to this approach in 2018.

3A – DATA OWNERSHIP COULD INTRODUCE INEQUALITY IN TERMS OF THE LEVEL OF PROTECTION FOR INDIVIDUALS

For the ordinary property regime to apply to an object, a market must exist such that the object is transferable and exchangeable at a price, or under any arrangement, freely determined by the parties. The same holds for data[37].

Under this framework, the major challenge is the data's price. Indeed, what is the price of a connection log, a fingerprint, photographs, a purchase or web-browsing history? Is this price the same regardless of the data subject? How is it determined? Academic research on the question of determining the price of personal data is still too recent to have been able to establish an accepted and recognized methodology[38].

Such uncertainty as to price has a dual effect: on the one hand, it increases the transaction costs, *i.e.*, the time and resources the individual needs to find a party who accepts to purchase his or her data at the price and on the terms he or she desires. These transactions costs increase all the more so as individuals have to negotiate separately with each potential buyer of their data, as Pamela Samuelson demonstrated (Samuelson, 1999, p.1135).

On the other hand, this uncertainty increases the risk of a disadvantageous agreement for the individual due to the asymmetry of information between the parties, meaning between the buyer, whose professional occupation is purchasing and using a large volume of collected data, and the data subject.

In order to overcome this difficulties, some authors have predicted the emergence of new intermediaries who are specialised in selling and renting data on the data subjects' behalf. These "*infomediaries* (Hagel III & Rayport, 1997)" would spare each individual from having to become a "*trader*" of his or her own data, while minimising the risks of disadvantageous agreements. Indeed,

37 The fact that data is perceived as "*free*" raises significant theoretical difficulties in the construction of a market and the analysis of competition on this market. *See* Eben, (n 39), p. 231.

38 As stated by Eben, "Studies on the value of data are fairly recent and the research on the topic is still in its infancy. The economic use of personal data is a growing business with a lot more room for research", (n 39), p. 246.

> *"consumers won't have the time, the patience, or the ability to work out the best deals with information buyers on their own. In order to help them strike the best bargain with vendors, new intermediaries will emerge".*

It follows from the foregoing that proponents of applying the property regime to data underestimate the prerequisites necessary for the very existence of trades. Indeed, a market is also a legal construct, with its institutions and legal safeguards. If this infrastructure does not exist, granting a right of ownership to property, even if involving data, would be ineffective and no trading would take place. Few commentators have seriously considered the nature and technicalities of the infrastructure required to operate a system based on the right of data ownership.

60

Kenneth Laudon (Laudon, 1996, p.92) has devoted the most work to this. He proposes the creation of a regulated national information market that would allow individuals to determine how many personal data they wish to sell by establishing a data account. Considering his own position, a such National Information Market (NIM) would allow

> *"[...] personal information to be bought and sold, conferring on the seller the right to determine how much information is divulged: Individuals would first establish information accounts and deposit their information assets and informational rights in a local information bank, which could be any local financial institution interested in moving into the information business. The banks would then pool these information assets and sell 'baskets' of them in a National Information Exchange. Buyers would receive the right to make commercial uses of personal information in those baskets for stated periods of time, in exchange for compensation".* *(Laudon, 1996, p.96)*

The contents of this account would be deposited with information banks. This new type of banks would group together the data deposited in the accounts, they would create baskets of data they would then sell to interested buyers in exchange for compensation. This compensation would be paid to the data subjects and the amount of compensation would be based on their contribution to such basket. Kenneth Laudon also proposes creating a unique identifier that would help individuals keep track of how their data are used. He proposes a substantial role for

government oversight and control. However, this proposal remains far from the reality of personal data law in Europe.

Génération Libre's proposals are undoubtedly based in part on Kenneth Laudon's work, in particular when they contemplate recognising individuals as "*database producers*[39]" who would register themselves with the French Data Protection Agency (CNIL). Data subjects would have a data platform manager exploit their data for specific purposes in order to receive income from them (Génération Libre, p. 92). However, these proposals address neither the issue of the cost of these platform managers (management fees assumed by data subjects) nor the issue of determining the price of the data. Nor do they address the correlative issue of the risks of disadvantageous transactions for data subjects resulting from the situation of information asymmetry.

61

In that regard, the EU Commission DGA draft represents an interesting and innovative piece of legislation to address some of these shortcomings. Indeed, the DGA creates a new category of *"data sharing"* providers (also called *"data intermediaries"*) that, when offering services to data subjects, shall *"assume fiduciaries duties"* and act in their *"best interest when facilitating the exercise of their rights, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses* (DGA, Art.11 §)*."* The DGA also sets out the requirements for the functioning of *"the competent authorities designated to monitor and implement"* the data-sharing service providers and entities *"engaged in data altruism"*. It also contains provisions on the right to lodge complaints against the decisions of such bodies and on the means of judicial redress (DGA, Chap. V).

As stated by recital 22 of the DGA, data intermediaries

> *"are expected to play a key role in the data economy, as a tool to facilitate the aggregation and exchange of substantial amounts of relevant data. Data intermediaries offering services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialized data intermediaries that are independent from both data holders and data users can have a facilitating role in the emergence of*

39 Within the meaning of Art. L.341-1 and Art. L.341-2 of the French Intellectual Property Code.

new data-driven ecosystems independent from any player with a significant degree of market power".

Once again, competition objectives interplay with data subjects' empowerment, just like with the right to portability introduced by the GDPR.

Similarly, the introduction of a right of ownership to data and the creation of the related market should have a mechanical consequence of facilitating transactions and, therefore, increasing the volume of trades made on this market. This increase in volume traded could in turn lead to more data accumulation by certain players. This is why, as Julie Cohen argues, "*[r]ecognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy* (Cohen, p.1391, 2000)."

One of the justifications for introducing a right of ownership to an object is that it makes it possible, through the market, to allocate scarce resources. Indeed, the intrinsic value of a medium of exchange is often a result of the scarcity or the utility of its composing object. If finite and highly desired, then the object (personal data for instance) will reach a high value (Harris, 1757). However, what seems rare today is not the data, but the protection of the data themselves. Yet, it is far from being established that introducing a right of ownership contributes to an increase in the level of data protection. Quite to the contrary.

Indeed, as Paul Schwartz explains (Schwartz, 2003-2004, p.2084), data protection can be considered as a public good, an aspect that proponents of data propertisation quite often neglect. In economic theory, a public good is, by definition, a "non-rival" and "non-exclusive" good. Such is the case of air quality or national defence, which are public goods « par excellence »: they benefit everyone without one person consuming them affecting the quantity of these same goods available for others. The same goes for data protection. However, the attributes of public goods are the opposite of goods that are private property, which in essence carries with it the right to exclude and, therefore, presupposes the existence of a rival good.

Applying the ordinary-law property regime to personal data, and, therefore, transforming them into something that is subject to a full right

of ownership, is likely to lead to individual practices that are prejudicial to people and erode the collective protection level (public good). By way of illustration, if personal data can be sold and transferred freely, then the collection of "*sensitive*" data, such as health, genetic or religious data, will, in principle, no longer be prohibited as it is the case today under the GDPR (GDPR, Art.9). In principle, collection of these data will be authorized. And it is their price on the market that, attesting to their scarcity or value, will determine how and in what quantities they will be put into circulation. This would lead to the dismantling of European's personalist approach towards data protection.

If sensitive data have a high price, it is also possible that the level of data protection enjoyed by individuals would then be very directly connected to their level of income. Indeed, the better off individuals are financially, the less they will need additional income from the sale of their sensitive data. As Valérie Peugeot, Commissioner with the CNIL explains, "[i]*f we monetize our data, we will create digital inequality*[40]." As Stacy-Ann Elvy (Elvy, 2017, p.1405) recently demonstrated, the risks created by data monetisation are particularly high for low-income social categories and minors and tenants. According to her, the risks of unequal access to the right to data protection generated by data-propertisation and direct-compensation (to individuals) models are as high as those resulting from models that advocate for payment for the right to data protection (Elvy, 2017, p.1405)[41]. Whichever model is chosen the practices allowed by these two models would be particularly harmful to individuals and a factor contributing to inequality between them. As a result, the two models would undermine the collective well-being represented by a high and equal level of data protection for all.

From an economic standpoint, application of the right of ownership to personal data is likely to bring about the following threefold perverse effect: (i) an increase in the incentive for companies to carry out transactions and accumulate data, a phenomenon that runs counter to the fundamental principles of data protection, proportionality and the minimising of data collection; (ii) legitimisation by the market, via the variation in the level of data prices, of data collection and uses that are

40 Quoted by the review Expertises, Mar. 2018, p. 82.

41 /Elvy distinguishes between competing models: the PDE ("personal-data-economy") model, which directly compensates individuals who accept to sell their rights; and the PFP ("pay-for-protection") model, which proposes to require payment for the right to data protection. The undesirable effects of these two models, although conceptually quite distant, are surprisingly similar.

now prohibited in Europe precisely because of the risk they carry for individual rights and freedoms; and lastly, (iii) an increase in inequality between individuals and the risk of transforming data from a non-rival good to a rival good, which would be drastically contrary to the objectives of encouraging innovation, even though the proponents of data propertisation have put forward these objectives.

3B – OWNERSHIP OF DATA OR THE "ILLUSION" OF INCREASED CONTROL

From a legal standpoint, application of civil ordinary law on ownership of property to personal data raises two main problems:

The first problem is related to the practical consequences of the unconditional transferability of *usus*, *fructus* and *abusus* to a third party and the subsequent use the third party may make of the data acquired. The issue of subsequent uses of data sold has long been the main limitation to the applicability of the right of ownership to data. As Pamela Samuelson illustrates, "*[a]n individual may be willing to sell his data to company N for purpose S, but he may not wish to give N rights to sell these data to M or P, or even to let N use the data for purposes T or U* (Samuelson, 1999, p. 1138)."

As stated by Stacy-Ann Elvy, the monetisation of personal data, which the author named as the "Pay for Data Economy" model (PDE), may provide to the consumers the *"illusion of control and choice"*. However, the lure of compensation and discounts, even if minor, may outweigh considerations regarding potential purchasers of consumer data and subsequent data usage[42]. In addition, the companies involved in the PDE may simply provide "take it or leave it" terms and conditions and privacy policies which will deprive the users of the ability to negotiate them. As an ICO official cautioned, one must be careful not to raise false hopes about the benefits that would result from hypothetical "ownership" of data as appearances can be misleading (Partovia, p.26, 2018)[43].

42 "Consumers who choose to participate in the PDE marketplace may not grasp the extent to which their data can be subsequently monetized once it is disclosed or transferred and how the data can be used by companies to make inferences about their lives and impact the opportunities they receive. Consumers may be unlikely to impose use restrictions on data transferees, such as prohibiting data analytics and generating inferences or review the terms and conditions and privacy policies of a company accessing their data to determine what will happen to their data after transfer or disclosure", Elvy, (n 91), p. 1415.

43 "Rather than trying to define data ownership as a legal concept, perhaps it should be viewed more as a philosophy for processing personal data. If an organisation instils a culture within the organisation where data belongs to a person and that person owns the data, it's a good starting point for building better relationships with customers. This won't fit all organisations, so you should be careful in giving data subject's false expectations." Discussion at the British Academy, Royal Society and TechUK seminar on the 3rd of October 2018, p. 26.

Here we realize how protective the principle of purpose specification and the prohibition against "*incompatible*" subsequent processing with the initial purpose provided for in the GDPR (GDPR, 1995 Art.5,) are for the rights of individuals.

In addition, as stated by Sarah Worthington, "*property is not as protective as one might think* (Worthington, p.11)." Indeed, it is important to note *"that rights, entitlements and the power to control need not necessarily be associated with ownership". The right to light is not associated with ownership of light, and control over the export of national art treasures does not indicate that the government owns all these art treasures. If rights and entitlements are identified as valuable, they can be allocated and protected without any intermediating notion of 'property ownership.'"*

Furthermore, if the data are definitively sold or even resold, how can we request that errors be rectified or changes be taken into account if the data are inaccurate or out of date since the data subject has no longer any rights on his/her personal data? These problems have led Paul Schwartz to propose a right of ownership to data with a power of "*partial" or "hybrid alienability*"(Schwartz, 2003-2004, p. 2095 et s.). Failing introduction of this type of limitation, individuals' right of ownership to their data could ultimately mean that they would be totally stripped of any control over their use, an effect that is paradoxical to say the least, since the primary objective of proponents of data propertisation is in fact to strengthen individuals' control. The current situation under the GDPR regime is more protective, even for subsequent sharing of data, since sharing does not mean the loss of the possibility for the individual to exercise his or her rights (Custers & Ursic, 2016, p.11)[44].

The second problem involves the issue of data transferability. Logically, if civil ordinary law on property were to apply to data, then the data would become transferable after the death of the person to whom they are related. The French Parliament[45] took a step in this direction by providing that individuals must be informed of their right to provide instructions on their personal data after their death. However, this "post mortem" right

44 "Data sharing does not imply that a data subject surrenders his or her data subject rights. When you sell your car, you no longer own your car. With personal data this is different, since each time a data subject chooses to share or disclose personal data, he still owns a version of the data (although it is difficult to dub this as the 'original data'). Data sharing does not affect a data subject's rights regarding the control over his personal data. However, as discussed above, in practice it may imply that it is less transparent for a data subject which data controllers process his personal data and for which purposes."

45 Amending of Art. 32 (6°) of the Act of 6 January 1978, as amended, introduced by the Act for a Digital Republic of 7 October 2016.

remains attached to the data subject and in no way implies the automatic transferability of his or her data to his or her heirs and assigns. It is, therefore, more a question of the data subject demonstrating control and exercising rights to his or her data than it is a question of exercising a right of ownership to the given data as transferable property. As Cécile Pérès rightly observes, the system adopted by the act "*suffers from the discrepancy between, one the one hand, the personalist dimension of the rights recognized for the data subject while alive vis-à-vis the controller, on the other hand, the lure of inheritance rights in order to ensure transmission* (Pérès, 2016, p.90)." In addition, the rules of law in force consider the right to one's image or the right to personal data protection as extra-economic rights. As such, they are non-transferable and the right to privacy ceases to exist with the individual's death[46].

CONCLUSION:

From both an economic and legal standpoint, it has not been established that propertisation of personal data leads to increased control by individuals over how their data are used or to improvement in collective well-being. The theory in favour of personal data propertisation assumes a debatable equivalence between the data subject's control over the use made of his or data and their ownership. However, an individual's ownership of data does not lead to more control over their use, quite to the contrary. Conversely, more control by individuals over the use of their data does not require the introduction of a right of ownership to such data.

At the other end of the spectrum, the calls for sharing these data, now directed toward companies, in particular through the introduction of the concept of data in the general interest, are based, on the assumptions, on the one hand, that data are rare, concentrated and, on the other hand, that it is their available volume which is the relevant criterion. In addition to the fact that this scarcity is debatable, this approach favours "quantitative" criteria to the detriment of an analysis of the systemic and legal prerequisites conducive to innovation and competition. The so-called "sandbox" initiatives taken by some regulators, such as the ICO, demonstrate that the links between the legal framework applicable to

46 The rules of law already in force recognise, through the devolution of the author's moral rights, an example of transferability of personality rights after the individual's death. However, the continued existence of this moral right depends on the existence of a work. As we have seen previously, it is difficult to consider a great number of personal data as works of art.

data protection and innovation are not always necessarily and unconditionally conducive to innovation. And the possible introduction of data in the general interest will do nothing to change this.

BIBLIOGRAPHY

U.S. Sen.Kennedy, Own Your Own Data Act. S.806, Mar.14.2019

French Civil Code, https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070721/

Loi n° 98-536 du 1 juillet 1998 portant transposition dans le code de la propriété intellectuelle de la directive 96/9/ CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données

Act No. 2016-1321 of 7 October 2016 for a Digital Republic

FRENCH COUNCIL OF STATE, 30 May 1930, *Chambre Syndicale de Commerce en Détail de Nevers*

FRENCH SUPREME COURT, Crim. Ch.., 20 May 2015, appeal No. 14-81336

Charter of Fundamental Rights of the European Union, OJ C 326/02, 26.10.2012

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28

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), *OJ L 119, 4.5.2016, p. 1–88*

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), *OJ L 157, 15.6.2016, p. 1–18*

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56–83

EUROPEAN PARLIAMENT AND OF THE COUNCIL, Proposal for a regulation of the european parliament and of the council on european data governance (Data Governance Act), COM/2020/767 final

EUROPEAN COMMISSION, *« Vers un espace européen commun des données », (25 April 2018), COM 232 final, p. 11*

EUROPEAN COMMISSION (2020), *"Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest"*

EUROPEAN COMMISSION (2020), "*A European Strategy for Data*"

Gotlieb v. Tropicana Hotel & Casino, 109 F . Supp. 2d, 324, 329, (E.D. Pa. 2000)

DELOITTE (2017), *Content & Technology*, Final report prepared for the DG Communications Networks

INSTITUT MONTAIGNE, (2015) "*Big Data and Connected Things*" https://www.institutmontaigne.org/en/publications/big-data-and-internet-things

GÉNÉRATION LIBRE (2018), *Les Data Sont à Moi* [*Data are Mine*], report

INFORMATION COMMISSIONER'S OFFICE, *Your Data Matters*, https://ico.org.uk/your-data-matters/

FRENCH AND GERMAN COMPETITION AUTHORITIES (2016), "*Data and competition Law*"

Julie COHEN (2018), "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review*, 2000, p. 1391

Lucie CLUZEL METAYER (2016), "Les Limites de l'Open Data" [The Limits of Open Data], AJDA p. 104

Bart CUSTERS and Helena URSIC (2016), "Big Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection", *IDPL*, Vol. 6, No. 1, p. 11

Lothar DETERMANN (2018), "Legal Studies Research Paper Series", Hasting College of the Law, Paper No. 265

Magali EBEN (2018), *Market Definition and Free Online Services: the Prospect of Personal Data as a Price*, Journal of Law and Policy, 14, p. 240

Tracy-Ann ELVY (2017), "Paying for Privacy and the Personal Data Economy", *Columbia Law Review*, vol. 117, nº. 6, Oct. 2017, p. 1405 et s.

John HAGEL III & Jeffrey F RAYPORT (1997), "The Coming Battle for Customer Information", *Harvard Business Review*

70

John HAGEL III and Jeffrey F. RAYPORT (1997), "The Coming Battle for Customer Information", *Harvard Business Review*

Joseph HARRIS (2020), " An essay Upon Money and Coins", dans Edward W fuller (dir.), *A Source Book on Early Monetary Thought,* Part I, Theories of Commerce, Money and Exchanges, 36, (1757-58), Economics, p. 283-288

Sam HARRISON (2018), "*Can You Make Money Selling Your Data?*", BBC's website

Neelie KROES (2013), "*The Economic and social benefits of big data."* Speech given at Webcast Conference on Big Data, Brussels, available online at http://europa.eu/rapid/pressrelease_SPEECH-13-450_en.htm

Jaron LANIER (2018), "*Should we treat data as labor? Moving beyond "free"*", AEA Paper ans Proceedings, nº 108, p. 38-42

Kenneth LAUDON (1996), *Markets and Privacy*, Comm. ACM, points 92-100

Lawrence LESSIG (1999), *Code and Other Laws of Cyberspace,*

Lawrence LESSIG (1999), *The Architecture of Privacy*

John LOCKE (1690), *Treatise of Civil Government*

Viktor MAYER-SCHÖNBERGER and Thomas RAMGE (2018), *A Big Choice for Big Tech: Share Data or Suffer the Consequences*, Foreign Affairs, p. 48

Fabrice MATTATIA and Morgane YAÏCHE (1995), « Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de

propriété ? » [Being the Owner of Personal Data: Can One Use Traditional Ownership Regimes?], *LRDI*, No. 114, p. 2

Thomas W. MERILL (1998), "The Right to Exclude there is more that just 'one of the most Essential Constituents of Property', it is the sine qua non", *Nebraska Law Review*, *Property and the Right to Exclude* 77, p. 730

Yann PADOVA (2014), "what the European Draft Regulation on Personal Data is going to change for companies?", *International Data Privacy Law*, vol. 4, Issue 1, p. 39–52

Romin PARTOVIA, ICO, "Reflections on the data ownership, rights and controls seminar from the ICO" *British Academy*, Royal Society and TechUK, seminar on the 3rd of October 2018 2018, p. 26, https://royalsociety.org/~/media/policy/projects/data-governance/data-ownership-rights-and-controls-October-2018.pdf

Cécile PÉRÈS (2016), « Les Données Personnelles et la Mort, Observations Relatives au Projet de Loi pour une République Numérique » [Personal Data and Death, Observations About the Bill for a Digital Republic]. *Recueil Dalloz*, p. 90

Nadezha PURTOVA, "Default entitlements in personal data in the proposed Regulation: informational self-determination off the table …and back on again?", Computer Law&Security Review, 30, Issue 1

Jeffrey RITTER and Anna MAYER (2017-2018), "Regulating Data as Property: A New Construct for Moving Forward", *Duke Law & Technology Review*, vol. 16, p. 261

Jeffrey RITTER, Anna MAYER (2017-2018), "Regulating Data as Property: A New Construct for Moving Forward", Duke Law & Technology, Vol. 16, p. 268

Teresa SCASSA (2018), "Data Ownership", *CIGI Papers*, nº. 187, p. 1

Paul SCHWARTZ (2003-2004), *Property, Privacy, and Personal Data*, Harvard Law Review, nº. 117, p. 2056 et s.

Carl SHAPRIO and Hal VARIAN (1997), *US Government Information Policy*, point 29

Pamela SAMUELSON (1999), *Privacy as Intellectual Property*, Stanford Law Review, vol. 52, p. 1125 et s.

Peter SWIRE & Robert LITAN (1998), None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive 8,

Cédric VILLANI (2018), *Donner un Sens à l'Intelligence Artificielle, pour une Stratégie Nationale et Européenne* [Giving Meaning to Artificial Intelligence for a National and European Strategy] - Report, p. 14, https://www.vie-publique.fr/sites/default/files/rapport/pdf/184000159.pdf

Sarah WORTHINGTON (2018), *Data Ownership, Rights and Controls: Reaching a Common Understanding. Discussions at a British Academy, Royal Society and techUK Seminar,* (contribution paper)

Sarah WORTHINGTON, "Legal Notion of Property and Ownership" British Academy, Royal Society and TechUK seminar 3 october 2018, p. 11 https://royalsociety.org/~/media/policy/projects/data-governance/data-ownership-rights-and-controls-October-2018.pdf

"The stakes of Open data policies", [les enjeux de l'Open Data"] AJDA, 2, 2016