The commodification of our digital identity: limits on monetizing personal data in the European context

Milena Mursia, Carmine Andrea Trovato

Abstract

Personal data have an immense economic value and are used by firms to power their business models. However, this fact is insufficient to argue that personal data can be lawfully traded on the market, similarly to a commodity. The extent to which personal data can be traded and monetized is the object of an intense debate. The aim of this paper is to explore whether personal data can be considered a counter-performance in an agreement, that is exchanged on the market for products/services and/or money, assessing whether this perspective is consistent with the fundamental rights' nature of the right to the protection of personal data and with personality rights in Europe, and the limits under the European General Data Protection Regulation.

I dati personali hanno un immenso valore economico e sono utilizzati dalle società per alimentare i propri modelli di business. Tuttavia, questa circostanza non è in sé sufficiente per poter affermare che sia lecito quindi commercializzare i dati personali sul mercato, analogamente a una merce. Il limite entro cui i dati personali possono essere scambiati e monetizzati sul mercato è oggetto di un intenso dibattito. Lo scopo di questo lavoro è esplorare se i dati personali possano essere considerati una contro-prestazione contrattuale, cioè se possano essere scambiati sul mercato per prodotti/servizi e/o denaro. Viene valutato se questa prospettiva sia coerente con la natura del diritto alla protezione dei dati personali quale diritto fondamentale e con i diritti della personalità in Europa, e quali siano i limiti imposti dal Regolamento Generale sulla Protezione dei Dati.

Table of contents

[*] Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Keywords

Data monetization - personal data - personality rights - GDPR – counter-performance

1. Introduction

Personal data have an immense economic importance in today's digital economy. The European Commission estimated in 2017 that the value of personal data in Europe might grow to approximately Eur 1 trillion annually in the following three years.[1]
Personal data are being commercialized and monetized by companies whose business models are centered on processing them. Such companies often provide products/services at "zero-price" in exchange of individuals' personal data.[2] For example, according to a Wall Street Journal analysis, the most popular Facebook apps gather volumes of personal data from users and their friends (on birthdays, sexual preferences, work history, education), and use them to attract advertisers, app makers, to show targeted ads or sell them to third parties.[3] Therefore, individuals "pay" in personal data by providing information about themselves.[4] Other companies purchase personal data directly from individuals (so-called "personal data economy models").[5] Indeed, apps such as Datum, Wibson, Datacoup, Ocean Protocol, Weople, advertise the possibility for users' to retake control of their personal data by selling them and prompt individuals to have a cut of the sale of their personal data.[6] In addition, other companies require users to pay a (higher) price in order to avoid the collection of personal data for advertising purposes (so-called "pay for privacy models").[7] The theoretical assumption that «allows and underpins such mechanisms is the construction of a "user-centric" economic system of personal data that conceives the individual as an owner of a wealth that can be shared».[8]
Thus, personal data are being commercialized on the market like a commodity[9] and it

[1] European Commission, Fact Sheet - *Questions and Answers – Data protection reform package*, 2017, accessed 26 June 2020.

[2] Organisation for Economic Cooperation and Development ("OECD"), *Quality considerations in digital zero-price markets. Background note by the Secretariat*, 28 November 2018.

[3] J. Angwin – J. Singer-Vine, *Selling You on Facebook*, in *wsj.com*, 7 April 2012.

[4] *Ibid.*

[5] S. Elvy, *Paying for privacy and the personal data economy*, in *Columbia Law Rev.*, 117(6), 2017, 1369 ss.; V. Ricciuto, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato* in N. Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milan, 2019, 128-129.

[6] G. Barber, *I Sold My Data for Crypto. Here's How Much I Made*, in *wired.com*, 17 December 2018; I. de Michelis di Slonghello – L. Bolognini, *An Introduction to the Right to Monetize (RTM)*, in *istitutoitalianoprivacy.it*, 9 April 2018, suggest introducing a right of monetization of individuals' personal data.

[7] S. Elvy, *Paying for privacy and the personal data economy*, cit., 1369.

[8] V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in *Diritto dell'Informazione e dell'Informatica,* 4, 2018*,* 718.

[9] V. Janecek – G. Malgieri, *Data Extra Commercium*, in S. Lohsse - R. Schulze - D. Staudenmayer (eds.), *Data as Counter-Performance—Contract Law*, Berlin, 2019.

is an established fact that they do have an economic value. Indeed, this has also been confirmed in different occasions by the Italian Competition and Market Authority ("AGCM"). For instance, in declaring the unfairness of certain contractual clauses provided for in the standard terms of WhatsApp, the AGCM has recently recalled in support of the solution adopted the «well-established orientation of the European Commission to recognize the nature of non-pecuniary counter-performance of the personal data of social media users, both in terms of consumer protection and in the assessment of mergers between companies. Such economic value is therefore suitable to configure the existence of a consumer relationship between the Professional and the user».[10] Also, the AGCM with decision of 29 November 2018 no. 27432, in considering that Facebook Ireland Ltd. and its parent company Facebook Inc had infringed the Italian Consumer Code by engaging in the misleading practice of emphasizing the "free" nature of the service, while the personal data collected was instead being used for commercial purposes, recognized the existence of a commercial transaction between Facebook and the users and thus an exchange of performances in the use of the social network.[11] Moreover, the fact that personal data are supplied by consumers as a sort of "payment" for digital services and digital content has also been recognized by the EU legislator in Directive 2019/770[12] and Directive 2019/2161[13] (see Paragraph 4 below in this respect).

That said, the acknowledgment of the economic value of personal data and that personal data can be traded in exchange for products and services does not in itself justify commodification of personal data. Indeed, whether and the extent to which personal data can be traded and monetized has been the object of an intense debate.[14] On the one hand, the tradability of personal data raises concerns given the EU's fundamental right of data protection and its nature; on the other, it is arguable that individuals should have the right to control their personal data[15] to a point where they can

[10] Autorità Garante della Concorrenza e del Mercato, *Decision CV154*, 11 May 2017; G. D'Ippolito, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Il diritto dell'informazione e dell'informatica,* 3, 2020, 634-674. The Authority's decision follows the position expressed by the national authorities responsible for the enforcement of consumer protection legislation in Common position of national authorities within the "CPC Network concerning the protection of consumers on social networks", 17 March 2017, which call for careful consideration of the possible unfairness of certain clauses contained in the general conditions drafted by the operators of social networks.

[11] See also decision of *Tar Lazio* (Administrative Court of Lazio), 10 January 2020, no. 261/20, which partly upheld the decision of the AGCM and reiterated that personal data are considered as an economic asset, and thus consumers «must be made aware of the exchange of performances» in the use of the social network.

[12] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJL136/1 ("Directive 2019/770").

[13] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7 ("Directive 2019/2161").

[14] J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, in *twobirds.com,* August 2019.

[15] European Commission, *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation* COM (2020) 264 final.

decide to "pay" with their personal data or otherwise dispose of them. In essence, the fundamental right to data protection should be balanced with other interests and fundamental rights, such as the free flow of data and the freedom to conduct a business and to contract[16] or have control over personal interests under principles of personal autonomy.[17]

The aim of this paper is to explore whether personal data can be exchanged for valuable assets (for example, products/services, other incentives) or money. In other words, can the processing of personal data be considered a counter-performance in an agreement and can individuals receive consideration in exchange of their personal data (the so-called data dividend)[18] - both acts resulting in personal data commercialization and monetization? The focus of the analysis will be Europe, in particular, the approach to data protection of the Council of Europe and the European Union.

Paragraph 2 will briefly analyse the personal data-centered business models and their related benefits and disadvantages for users. Paragraph 3 comprises two sub sections, the first sub of which will explore whether the commodification of personal data is consistent with the nature of the right to the protection of personal data. Thus, it will examine the fundamental right to data protection enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR")[19] and the Charter of Fundamental Rights of the European Union ("Charter")[20], and the dual nature of personal data, as a projection of an individual's personality and as an economic good.[21] The second sub section then will investigate whether and how[22] personal data can lawfully be traded under the General Data Protection Regulation ("GDPR")[23], having regard to the relevant opinions of the European Data Protection

[16] Garante per la protezione dei dati personali, *Relazione annuale 2019*, 23 June 2020, 124-125.

[17] N.R. Koffeman, *(The right to) personal autonomy in the case law of the European Court of Human Rights*, in *scholarlypublications.universiteitleiden.nl*, June 2010, citing the European Court of Human Rights ("ECtHR") case law, according to which personal autonomy (or self-determination) is considered both a principle of law «underlying the interpretation of the ECHR guarantees» (*Pretty v The United Kingdom* (2002) 35 EHRR 1, § 61), and a right itself, as a component of the right to a private life under Article 8 European Convention for the Protection of Human Rights and Fundamental Freedoms (*Evans v The United Kingdom* (2008) 46 EHRR 34, § 57). In *Pretty,* § 62, it is defined as «the ability to conduct life in a manner of one's own choosing»; P. De Hert – S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action* in S. Gutwirth – Y. Poullet – P. de Hert (eds.), *Reinventing data protection*?, Dordrecht, 2010, 14-15. Moreover, H. J. Snijders, *Privacy of Contract* in K. Ziegler (ed.), *Human Rights and Private Law: Privacy as Autonomy*, Oxford, 2007, 108: «personal autonomy can be concretised as the right to freely enter into contracts».

[18] Garante per la protezione dei dati personali, *Relazione annuale per il 2018. Discorso del Presidente Antonello Soro*, 7 May 2019.

[19] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended), Rome, 4 November 1950.

[20] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

[21] *Diritto mercato e tecnologia*, interview with G. Finocchiaro, *La nuova sovranità privata e l'ambivalenza del dato personale. Intervista a Giusella Finocchiaro*, in *blogstudiolegalefinocchiario.it*, 3 December 2019.

[22] F.G. Viterbo, *Freedom of contract and the commercial value of personal data*, in *Contratto e impresa Europa,* 2016, 593 ss., 596.

[23] 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)

Supervisor ("EDPS") and the European Data Protection Board ("EDPB") and certain decisions of the national data protection authorities and courts. More specifically, it will evaluate whether the legal basis of consent and contract (respectively Articles 6(1)(a) and 6(1)(b) GDPR) can justify the tradability of personal data.[24]
This paper will conclude that the nature of data protection as a fundamental right and as a personality right does not *per se* exclude the alienability of personal data, however this is limited to the conditions of the GDPR. In this regard, it shows that there is room to interpret the legal bases under Article 6 GDPR in ways that could allow the commercialization and monetization of personal data.

2. The commercial use and monetization of personal data

Several business models are based on the collection and analysis of users' personal data;[25] these monetize personal data[26] and generate revenues. More specifically, personal data are used by companies for a variety of commercial purposes, some concern direct monetization through the sale of personal data, others indirect monetization, such as for security, product/service improvement and development, improvement of the customer experience, including a personalized customer experience.[27] One important use of personal data consists in the collection of users' interests, preferences or other characteristics to place targeted online advertising, which funds a considerable number of online services.[28]
Here, personal data-centered businesses will be divided into three models: (i) zero-price[29]; (ii) personal data economy[30]; (iii) pay for privacy.[31] This section will describe these, in turn, highlighting some of the benefits and disadvantages for the users deriving from the collection and use of their personal data[32] - some of which, as examined in the following sections – have influenced the legal position on the alienability of

[2016] OJ L119/1.

24 V. Janecek – G. Malgieri, *Data Extra Commercium*, cit., 7.

25 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1371.

26 European Commission, *Commission Staff Working Document Impact Assessment Accompanying the document Proposals for Directives of the European Parliament and of the Council (1) on certain aspects concerning contracts for the supply of digital content and (2) on certain aspects concerning contracts for the online and other distance sales of goods* COM(2015) 634 final: «Digital content may be supplied either against a price or against (personal and other) data provided by consumers as a counter performance…the great majority of contracts for the supply of digital content involve collection of data of an economic value, which can be monetised by the suppliers».

27 Competition and Markets Authority ("CMA"), *The commercial use of consumer data - Report on the CMA's call for information*, June 2015; J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 38.

28 CMA, *The commercial use of consumer data,* cit., 6.

29 OECD, *Quality considerations in digital zero-price markets,* 4.

30 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1369.

31 *Ibid.*

32 CMA, *The commercial use of consumer data,* cit., 7.

personal data.

As to the zero-price models, according to an economic theory the provision of personal data can be considered an implicit component of the price that the users pay for the purchase of the primary service[33] (typically, digital content[34] or digital service[35]). Such digital content/service is generally advertised as for free, while actually users provide their personal data in exchange.[36] Certain authors argue that, notwithstanding the fact that there is no trade of currency, this is still a real commercial transaction on the basis that «the argument that free goods are not sold […] does not make economic sense»[37] and that personal data are indeed the price users are paying.[38] The latter position, as demonstrated above, is also shared by the European Commission.

The personal data economy models are advertised as empowering individuals to obtain value from their personal data by selling or providing access to their personal data to data buyers.[39] For instance, certain apps allow individuals to earn value through direct marketing, profiling, personalized offers and by allowing third parties to enrich their databases with the account holders' personal data.[40]

Finally, paying for privacy models require individuals who do not want to consent to the collection of their personal data for targeted advertising/marketing purposes to pay (higher) fees for accessing the product/service, whose providers offer lesser charges/discounts to individuals who instead provide their consent for such purposes.[41]

Users, companies and the economy in general benefit from the collection and use of personal data.[42] From the users' point of view, the benefits concern personalised services, broader options, improvement of existing services, more pertinent advertising and offers that may reduce the search cost for users.[43] Also, the described business models increase the users' awareness of the value (broadly understood from a qualita-

---

33 Autorità Garante della concorrenza e del mercato, *Autorità per le garanzie nelle comunicazioni*, *Garante per la protezione dei dati personali*, "*Indagine Conoscitiva Sui Big Data*", 10 February 2020.

34 J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 36: «Digital content, in short, means data produced and supplied in a digital form. Forms of digital content may include computer programs, games, music, videos, applications, cloud storage and potentially social media».

35 According to article 2(2) of Directive 2019/770: «'digital service' means: (a) a service that allows the consumer to create, process, store or access data in digital form; or (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer», for example social media platforms and cloud computing services.

36 J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 36.

37 OECD, *Quality considerations in digital zero-price markets,* cit., 5.

38 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1385: data are not money or currency, but this label is used to describe the situation where individuals provide personal data to obtain zero-price products/services; J. Lanier, *You Are Not a Gadget: a Manifesto*, 2011.

39 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1375.

40 For instance Weople, described at *weople.space/en/#functions*.

41 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1387-1392.

42 CMA, *The commercial use of consumer data,* cit., 7.

43 P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, in *cerre.eu*, 25 January 2016; CMA, *The commercial use of consumer data,* cit., 50-51.

tive and quantitative point of view) of their personal data.[44]

However, it is questioned whether these business models are beneficial to individuals, as significant concerns arise in relation to data protection. First, users do not clearly know the ultimate value of their personal data and thus do not fully understand the extent to which they give away their personal data in exchange for "free" products/services or for other incentives.[45] For instance, the value of their personal data may exceed the value of the product/service they receive "for free".[46] Moreover, individuals may not be aware of and/or fully understand the use of their personal data.[47] This information asymmetry is also exacerbated by the use of nudging[48] and dark patterns[49], techniques exploiting users' psychological biases[50] that lead them to privacy intrusive choices and/or to share their personal data.[51] For example, when a user is offered the possibility to obtain a discount (or other "short-term financial benefit") in exchange of her consent to data processing, the real cost of this transaction is difficult to understand. Here, according to the research, as the short-term benefit (discount) is tangible and instant, while the potential give-away of privacy is long term and unrealized, the user will likely choose the short-term benefit. Also, users are more inclined to disclose personal data when they feel they are "in control" of them (so-called "control paradox"). However, control is often not effective as users are manipulated through dark patterns.[52]

---

44 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1393.

45 S. Athey – C. Catalini _ C. Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, in *National Bureau of Economic Research Working Paper Series*, No. 23488, 2017. The paper investigates distortions in consumer behavior which may limit the ability of consumers to safeguard their privacy. Indeed, the effect small incentives have on disclosure may explain the privacy paradox: People say they care about privacy but are willing to relinquish private data to firms quite easily when enticed to do so through small incentives. In this study, students were offered a pizza in exchange for disclosure of some personal data.

46 Ivi, 1385.

47 OECD, *Quality considerations in digital zero-price markets,* cit., 25, according to an experimental study concerning a social networking service «74% of participants opted not to consult the terms of service, and 98% did not identify a provision that allowed the supplier to share data with employers and law enforcement agencies (Obar and Oeldorf-Hirsch, 2018)».

48 Norwegian consumer council, *Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*, in *edri.org*, 27 June 2018, 6. Nudging «describes how users can be lead toward making certain choices by appealing to psychological biases. Rather than making decisions based on rationality, individuals have a tendency to be influenced by a variety of cognitive biases, often without being aware of it».

49 Ivi, 7: dark patterns are identified when «deliberately misleading users through exploitative nudging»

50 Norwegian consumer council (n 43) 6: «individuals have a tendency to choose smaller short-term rewards, rather than larger long-term gains»; OECD, *Quality considerations in digital zero-price markets,* cit., 26-27, referring to the "free effect" with regard to the fact that «valuations for free goods are boosted beyond their benefit-cost differences» and to the "privacy paradox" referring to the fact that even though users consider privacy important, they tend not to make decisions with privacy in mind.

51 Norwegian consumer council, cit., 3.

52 Ibid. 32: for example, Facebook's GDPR popup «You control whether we use data from partners to show you ads» is misleading since users are not given substantial control over the data collection, but only the possibility to decide which ads they will see.

Nevertheless, despite the fact that personal data is fluid, intangible and dynamic[53], it is argued that it is economically possible to quantify its monetary value.[54] Indeed, not only do the above business models show this in different ways, but there are also various specific methods to calculate the value of personal data.[55] Moreover, the overall information asymmetry between individuals and entities processing personal data – both with regard to the value of personal data and the uses of personal data - could be addressed by making existing fairness and transparency rules more effective (both from a privacy point of view[56] and from a consumerist point of view[57]) and/or by introducing new ones, thus raising the awareness of individuals about their data processing.

In this last regard, it is suggested (and agreed with) that individuals should have a

[53] Competition and Markets Authority ("CMA"), *The CMA's Response to the UK Government's Call for Views on the Draft Directives on the Online Sales of Digital Content and Tangible Goods*, 15 February 2016; J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 37.

[54] J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 37; G. Malgieri – B. Custers, *Pricing privacy the right to know the value of your personal data*, in *Computer Law & Security Review*, 34(2), 2017, 289 ss.

[55] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, 2 April 2013, 18-32, identifies possible methodologies, one based on market valuation of personal data (in this case values can be derived from «financial results per data record», «market prices for data», «cost of data breach», «data prices in illegal markets») and one on individual's valuation of personal data, which focuses on «surveys and economic experiments», and «data on willingness of users to protect their data»; G. Malgieri, *Data Extra Commercium*, cit., 9-14: it is necessary to (i) clarify how to «express monetary value» of personal data, (ii) identify which object is priced and the pricing factors, and (iii) the pricing system («how to attach the value to the object»). As to (i) the value of personal data can be expressed in monthly terms, i.e., in terms of euro or dollars per month, and per person. As to (ii), the objects which are being priced are datasets and the factors affecting the price are «size, completeness, accuracy, being up-to date, rareness and uniqueness, and identifiability». Finally, the methods to determine the actual value of personal data in (iii) are various, some already identified by the OECD (see above) in market valuation and individual's valuation.

[56] Articles 5, 13 GDPR. According to F. Schaub - R. Balebako - A. Durty - L.F. Cranof, *A Design Space for Effective Privacy Notices,* Symposium on Usable Privacy and Security (SOUPS '15), Ottawa, Canada, Jul 2015. Other proposals at *usableprivacy.org/publications*. In recent years, some have begun to speak of «machine readable information notices», i.e., privacy notices that can be interpreted by a machine in a way that facilitates individuals' understanding of the complexity of how technologies work and how they continue to evolve. This could be a way of informing the data subject about compliance with all agreed conditions much more effectively than reading a textual information notice. We are still at the beginning of this process, but there are already concrete proposals to raise people's awareness.

[57] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJL 95/29 requires the use of plain, intelligible language. National investigations have addressed concerns of transparency and fairness in terms and conditions of websites and social media platforms. For example, the Autorità Garante della Concorrenza e del Mercato (Italian Competition and Market Authority), decision 29 November 2018 no. 27432, found that Facebook Ireland Ltd. and its parent company Facebook Inc infringed the Italian Consumer Code by engaging in the misleading practice of emphasizing the "free" nature of the service, while the personal data collected was instead being used for commercial purposes, thus considering this service as a commercial transaction between Facebook and the users; this decision was partly upheld by the *Tar Lazio* (Administrative Court of Lazio), 10 January 2020 no. 261/20, which stated that, given that personal data are considered as an economic asset, operators need «to comply with […] obligations of clarity, completeness and non - misleading information provided by the consumer protection legislation» and consumers «must be made aware of the exchange of performances» in the use of the social network.

right to know the quantitative value of their personal data.[58] More specifically, data controllers should inform individuals of the price of their personal data calculated on objective parameters.[59]

As to the additional drawbacks deriving from the application of these business models, it is also contended that these may determine unfair access to privacy and discriminatory behavior.[60] Indeed, privacy could potentially become a luxury available only to those who can afford it, while low-income users would accept subjecting themselves to an increased data collection, either for a discount, other benefit or remuneration.[61]

In contrast, other authors suggest that users are actually capable of deciding to trade their personal data "for convenience" and make their own choices on the related issues[62]; moreover these models could help users from different socio-economic contexts[63] and grant them a better control over their data as property rules would allow each individual to decide what information to disclose and protect «both those who value their privacy more […] and those who value it less».[64]

That being said, from an economic perspective individuals may indeed trade personal data and the protection of personal data similarly as a service and monetize them.[65] What remains unclear is the legal position on the lawfulness of such practices and the legal implications of recognizing them.[66] Indeed, the *Garante per la protezione dei dati personali* ("Italian DPA") has recently asked the EDPB to express an opinion on certain business models based on the commercialization of personal data, given the

---

58 G. Malgieri, *Data Extra Commercium*, cit., 14-16.

59 *Ibid.* Also, the new California Consumer Privacy Act of 2018, Civil Code §1798.100-1798.199 ("CCPA") and Title 11. Law Division 1. Attorney General Chapter 20. California Consumer Privacy Act Regulations §999.300-999.341 ("Proposed Regulations") provide that a business may offer financial incentives (i.e., «program, benefit, or other offering, including payments to consumers, related to the collection, retention, or sale of personal information») or a price or service difference to individuals for the collection of their personal data (CCPA §1798.125. (b)(1)). In such a case, individuals shall receive a «notice of financial incentive» which, among others, includes: «an explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: a) a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and b) a description of the method the business used to calculate the value of the consumer's data» (Proposed Regulations §999.307 (b)(5)(a)-(b)).

60 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1400-1406.

61 *Ibid.* see also Garante per la protezione dei dati personali, *Monetizzazione dati fra le sfide più delicate,* 5 October 2020: «*Ma i dati personali, prima che una risorsa economica, costituiscono un bene giuridico, oggetto di un diritto "di libertà" che come tale non può essere alienato. Una delle sfide più delicate riguarda proprio la monetizzazione dei dati. Se, infatti, si legittimasse la remunerazione del consenso al trattamento, si rischierebbe la rifeudalizzazione dei rapporti sociali, ammettendo che per necessità si possa essere disposti a cedere, con i dati, la propria libertà*».

62 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1404.

63 *Ibid.*

64 L. Lessig, *Code and Other Laws of Cyberspace*, New York, 1999; N. Purtova, *Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation*, in *European Journal of Legal Studies* 2010.

65 P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 6.

66 EDPB, *Minutes, 13th Plenary meeting*, 10 September 2019, received by the EDPB Secretariat with e-mail of 15 May 2020, includes as a point of discussion the «remuneration to data subjects/app users in exchange for their personal data».

controversial issue of the "merchantability" of personal data which are being attributed economic value.[67]
The next section explores the right to data protection to assess whether its intrinsic nature represents a limit to the merchantability of personal data.

3. The European right to the protection of personal data

The personal data monetization models described consider personal data as a "currency".[68] However, according to the EDPS, under EU law personal data cannot be reduced to a "mere economic asset", given the fundamental right's nature of the protection of personal data.[69]
The latter position is grounded in the natural law view that every human being is a bearer of innate rights that the State does not assign but simply recognizes. Therefore, as rights are inextricably linked to human nature, they are inviolable both by the State itself and by other citizens and cannot be reduced to a commodity.[70]
This section will explore data protection as a fundamental right and as a personality right to assess whether these qualifications determine a ban or restrictions on the merchantability of personal data.

3.1. Data protection as a fundamental right

"Privacy rights" in Europe encompass the right to the respect for private life (the "right to privacy") and the right to the protection of personal data.[71] These are protected as fundamental rights at European level and in national laws of EU Member States[72]: the right to privacy under Article 8 of the ECHR and Article 7 of the Charter, and the right to the protection of personal data under Article 8 of the Charter.
The right to privacy is considered an "opacity tool"[73] or a "defensive mechanism"[74], meant to protect one's personal sphere (to be intended broadly as covering the «home,

[67] Garante per la protezione dei dati personali, *Dati in cambio di soldi: il Garante privacy porta la questione in Europa. Sotto la lente dell'Autorità la app "Weople"*, 1 August 2019, concerning the request to the EDPB to express an opinion on "Weople"; however, the EDPB sent a letter to Weople, stating that the «request for an opinion […] was withdrawn by the Italian Supervisory Authority, and therefore the EDPB is no longer drafting such an opinion» [EDPB Secretariat, *Response to Hoda letter*, 21 January 2020].

[68] EDPS, *Opinion 8/2018 on the legislative package "A New Deal for Consumers"*, 5 October 2018.

[69] *Ibid.*

[70] See for example, J. Locke, *Two Treatises of Government,* Cambridge, 1988) and J. M. Finnis, *Natural Law and Natural Rights*, Oxford, 2011.

[71] P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 34.

[72] Ivi, 35-36.

[73] N. Purtova, *Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights*, in *Neth Q Human Rights*, 2010, 179 ss., spec. 182-183.

[74] Ivi, 180.

family life and correspondence, bodily integrity and decisional autonomy»)[75] from the intrusion and interference of others (the State, but also private parties).[76] On the contrary, the right to data protection is a «transparency tool»[77], «a dynamic kind of protection»[78], meant to give individuals control on how personal data are collected and used.[79] In this sense, personal data protection is broader than privacy because it addresses problems and needs underlying the processing of personal data regardless of their relationship with privacy[80] (i.e., need for transparency; automatic processing concerns), on the other, it is more narrow because it only concerns «the processing of personal information, with other aspects of privacy protection being disregarded».[81]

Based on these premises, certain authors have criticized the qualification of the right to data protection as a fundamental right, arguing that data protection interests might not justify restrictions to the freedom of contract of individuals[82], for example a prohibition to waive data protection rights.[83] In fact, the processing of personal data does not always relate to the private sphere of individuals and thus less fundamental interests are concerned.[84] However, this position is flawed as it does not take into account the evolution of privacy rights in Europe. Indeed, despite the two rights being different, they are related[85], as the right to the protection of personal data is considered intrinsic to the right to privacy under the ECHR.[86] The concept of privacy has progressively broadened - from the «right to be left alone»[87], to the right to maintain control over the flow of one's personal data and to determine how to shape «one's own private sphere».[88] Therefore, data protection in Europe is an autonomous fundamental right.[89]

That said, the fundamental right to data protection is not absolute and shall be balanced with other fundamental rights and interests. Indeed, according to the GDPR,

---

75 Ivi, 181.

76 Ivi, 187.

77 Ivi, 197.

78 S. Rodotà, *Data Protection as a Fundamental Right* in S. Gutwirth – Y. Poullet – P. de Hert (eds.) *Reinventing data protection?*, Berlin, 2010, 77 ss., spec. 79.

79 N. Purtova, *Private Law Solutions in European Data Protection,* cit., 197.

80 Ricciuto, cit., 103.

81 P. Hustinx, *EU Data Protection Law - Current State and Future Perspectives*, 9 January 2013.

82 N. Purtova, *Private Law Solutions in European Data Protection*, cit., 180.

83 C. Cuijpers, *A Private Law Approach to Privacy; Mandatory Law Obliged?*, 2007, 304, 312-313.

84 *Ibid.*

85 P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 34.

86 N. Purtova, *Private Law Solutions in European Data Protection*, cit., 181, recalling *I v Finland* (2009) 48 EHRR 31, §§ 35-36: «The processing of information relating to an individual's private life comes within the scope of Article 8».

87 S. Rodotà, *Data Protection as a Fundamental Right,* cit., 80 referring to the famous article of S. D. Warren – L. D. Brandeis, *Right to Privacy* in *Harv L Rev*, 4, 1891, 193 ss.

88 *Ibid.*

89 Article 16, Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 ("TFEU") now constitutes the legal ground for EU institutions to effectuate the right to data protection throughout the EU.

while the right to the protection of personal data should be «designed to serve mankind», «it must be […] balanced against other fundamental rights, in accordance with the principle of proportionality».[90] In particular, it refers to the fundamental right to the respect for private life[91] (which also includes the principle of autonomy/self-determination[92] and informational self-determination[93]) and the freedom to conduct a business (which also includes the freedom of contract[94]). Also, the GDPR, by ensuring uniform rules throughout the EU, pursues the economic interests related to the free movement of personal data[95], such as «the proper functioning of the internal market».[96] Such free movement of personal data shall not be «restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data».[97]

Moreover, it is arguable that the data subject in the GDPR also plays the role of a contractor and that the data subject's consent to data processing also indicates a willingness to negotiate. Otherwise, it would not be possible to explain Article 8(3) GDPR on the child's consent, which provides that paragraph 1 of the same article, setting the minimum age for a lawful expression of the child's consent, «shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child». If the European legislator had considered the consent to the processing of personal data totally unrelated to the discipline of contracts and merchantability, there would have been no need to save «the general contract law of Member States».[98]

Therefore, there is no dispute that the GDPR provides a dual approach[99] to the protection of personal data: on one side, it protects persons with regard to the processing

[90] Recital 4 GDPR.

[91] Article 7 Charter corresponding to Article 8 ECHR.

[92] See note 12 above.

[93] The ECtHR in *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (2018) 66 EHRR 8, § 137 found that informational self-determination is part of the right to private life. P. De Hert – S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg,* cit., 19: this is the capacity of the individual to «have control […] of the use of personal information»; A. Rouvroy – Y. Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* in S. Gutwirth - Y. Poullet – P. de Hert (eds.), *Reinventing data protection?*, Berlin, 2010, 45 ss., spec. 51-52: a libertarian and individualistic interpretation of the informational self-determination allows individuals to be empowered to a point where they can alienate their right to data protection.

[94] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17: Article 16 Charter "freedom to conduct a business" also covers the freedom of contract.

[95] Recitals 9-10 GDPR; A. Mantelero, *The Future of Consumer Data Protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics* in *Computer Law and Security Review*, 30, 2014, 643 ss.

[96] Recital 13 GDPR.

[97] *Ibid*; Article 1(3) GDPR.

[98] V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*", cit., 723.

[99] The need to balance the fundamental rights and the internal market economic considerations was also present in the 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 [1995] OJ L281/31, Recital 3, Article 1.

of their personal data, and on the other hand, other fundamental rights and interests, aiming at the free movement of personal data[100] throughout the EU Member States, underpinned by its harmonised level of protection there.
Personal data are thus protected both as aspects of one's identity and as economic goods subject to processing and circulation.[101] Hence, an interpretation of the fundamental right to data protection in light of the GDPR does not equate to a ban on the merchantability of personal data premised on an alleged preeminence of natural persons with regard to the processing of personal data.
On the contrary, it allows (and actually mandates) the balance of the need to protect natural persons with regard to the processing of their personal data and the need to encourage freedom of economic initiative and to conduct a business, as well as the development of new services necessary to guarantee pluralism and competitiveness of the digital single market.[102] Indeed, it is against this background that the recent Proposal for a Regulation European Data Governance should be read, which aims at fostering «the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU».[103]
One further step should be made in the analysis of the right to data protection, that is the deep connection between personal data and personhood.

3.2. Data protection as a personality right

The origins of data protection in Europe are founded in the framework of personality rights.[104] It is argued that personality rights origin from the right to privacy under Article 8 ECHR.[105] As mentioned, Article 8 ECHR progressively evolved from a negative right, providing protection from arbitrary interference, into a positive one; indeed, the scope of the right to privacy has gradually broadened and interpreted as a personality

[100] Article 1 GDPR; F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018.

[101] N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in Id. (ed.), *Persona e mercato dei dati,* cit., 35 ss., 91.

[102] Garante per la protezione dei dati personali, *Relazione annuale 2019*, cit., 124-125.

[103] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) [2020], COM(2020) 767 final 2020/0340 (COD).

[104] G. Resta, *I diritti della personalità*, in G. Alpa – G. Resta (ed), *Le persone fisiche e i diritti della personalità*, Torino, 2006, 361, 363, "personality rights" are a private-law category of civil law countries in Europe, originated from the German scholars of the nineteenth century; G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, in *Tulane European and Civil Law Forum,* 26, 2011, 34, this notion refers to a bundle of rights «aimed at the protection of the integrity and inviolability of the individual». In common law the concepts of privacy and defamation are the closest equivalents for the protection of non-economic interests of personality rights, while the right of publicity protects the economic interests.

[105] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"* in *Utrecht Journal of International and European Law*, 31(80), 2015, 25 ss. As to Article 7 Charter "right to private life", the Explanations of the Charter specify that «The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR», thus the reasoning should be the same.

right, covering the protection of all aspects of a person's identity and development[106], including «a positive freedom to control personal information».[107] As to the right to data protection, this too has its origin in Article 8 ECHR[108] and has evolved from a negative right, concerned with the obligations of data controllers[109], into a right that protects personal interests of individuals.[110] Thus, arguably, the right to data protection falls under the scope of personality rights.[111] More specifically, the right to data protection is directly related to the protection of human dignity (Article 1 of the Charter) and contributes to the «constitutionalisation of the person».[112] Personal data are linked to one's being, compose a person's digital identity as if it were a projection of the person herself, «a part of her».[113] Thus, data protection in Europe represents a tool for the protection and development of individual's personality.[114] This determines a less market-oriented approach to data protection in Europe compared to other legal systems, such as the USA.[115] Therefore, what needs to be explored is the extent to which it is possible to negotiate attributes of individuals' personality - personal data being intangible aspects.

Attributes of an individual's personality (surely intangible ones, for instance image and name) are in practice often exploited on the market[116], however the traditional position of private law scholars is to consider personality rights as absolute, inalienable and not

[106] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, cit., 44: a case falls under Article 8 ECHR when a person is affected in her «identity, personality or desire to flourish to the fullest extent». The right to privacy is interpreted «as a right that guarantees the development and expression of one's identity and personality» [*Biriuk v. Lithuania,* app no. 23373/03 (2008) § 38; *Varapnickaite-Mazyliene v. Lithuania*, app. no. 20376/05 (2012) § 43].

[107] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, cit., 44.

[108] Explanations of the Charter, cit.

[109] As provided by Article 4(7) GDPR, "data controller" means «the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law».

[110] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, cit., 46.

[111] Ivi, 26; H. Pearce, *Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law* in *Eur Data Prot L Rev*, 4, 2018, 190 ss., spec. 193.

[112] S. Rodotà, *Data Protection as a Fundamental Right*, cit., 80.

[113] G. Alpa, *La "Proprietà" dei dati personali*, in N. Zorzi Galgano (ed.), *Persona e mercato dei dati,* cit., 11 ss., spec. 17; J.E.J. Prins (Corien), *Property and Privacy: European Perspectives and the Commodification of Our Identity*, in *Information Law Series*, 16, 2006, 223 ss., spec. 234.

[114] S. Rodotà, *Data Protection as a Fundamental Right*, cit., 80.

[115] A. Mantelero, *The Future of Consumer Data Protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics,* cit., 11: a different approach more widely accepted in the USA is to grant individuals property rights over personal information; P. Schwartz, *Property, Privacy, and Personal Data,* in *Harv L Rev*, 2004, 2056 ss., spec. 2057 referring to scholars who, given personal data have become a commodity, «have advocated propertization of personal information» and the free alienability.

[116] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 42.

subject to the statute of limitations.[117] With regard to the monetization and tradability of personal data, the EDPS stated that «there might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation».[118] According to the writers, the traditional view and the EDPS' statement and analogy are not properly worked through and should be clarified by introducing proper distinctions. First, personality rights have both economic and non-economic aspects; for instance, with regard to intangible attributes, honor, privacy and personal identity represent personal non-economic values, while one's name, image and personal data are intangible expressions of a person, having an economic value.[119] The latter can be commercially exploited by third parties.[120] Secondly, it is necessary to distinguish between physical attributes of personality, such as one's body and body parts, and non-corporeal attributes, such as one's image, name and personal data. Only the physical attributes cannot be commercially exploited and form the source of profits.[121] One could argue in fact that only the exploitation of physical attributes of one's personality could endanger a person's integrity, the value of human dignity and the value of equality, as differences in wealth could negatively affect people's choice to dispose of their body.[122]. More simply, our society seems more open to accepting some forms of exploitation of incorporeal aspects of personal identity, including personal data. Indeed, this is also confirmed by legislation which provides different rules for physical and incorporeal attributes of personality; for instance, Article 3 Charter introduces a «prohibition on making the human body and its parts as such a source of financial gain»[123], while no similar ban is stated with

[117] G. Resta, *I diritti della personalità,* cit., 362.

[118] EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017 ("EDPS 2017").

[119] S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Turin, 2018, 16.

[120] Ivi, 17 and 80 referring to the intellectual property approach to justify the tradability of incorporeal attributes of personality. Regardless of the approach chosen, incorporeal attributes of personality have an economic and tradable content; G. Resta *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 42, 50 referring to the principle of personal autonomy which «lies at the core of the continental system of personality protection» and on which basis the courts have recognized that «every individual should have the right to freely decide who, under what conditions and for which purposes may lawfully exploit aspects of his/her personality».

[121] N. Zorzi Galgano (ed.), *Le due anime del GDPR e la tutela del diritto alla privacy*, cit., 63; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 20: physical attributes are subject to the principle of gratuitousness (they can be donated), thus in this sense they are off the market.

[122] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 58. An exception could be found in a person's hair, which instead can be sold; however, technically, hair is not a live part of a person's body and, anyhow, the commercialization for an economic return does not put a person's dignity or self at risk.

[123] A similar approach is adopted in Italy (Article 5 Civil Code: «acts of disposition of one's own body are prohibited when they cause a permanent damage in physical integrity, or when violate the law, public order or morality») and France (Article 16-1 and 16-5 Civil Code: «the human body, its elements, and its products may not form the object of a patrimonial right» and «agreements that have the effect of bestowing a patrimonial value on the human body, on its elements, or on its products are null»- translation is found at Légifrance-Catalogue des traductions, "Code civil" (21 December 2015). Specific rules govern clinical trials: the Regulation (EU) No 536/2014 of the European Parliament and

regard to personal data under Article 8.[124] Thus, if personal data do not fall within the non-patrimonial scheme typical of personality rights (especially physical attributes of personality rights), then personal data can be the object of negotiation. However, this does not mean that the freedom to contract intangible aspects of personality is not subject to any limitation. Indeed, intangible attributes of personality rights can be traded and exploited by third parties with individuals' consent, but they cannot be waived[125], the commercial transaction is subject to restrictive interpretation[126] and consent is always revocable.[127] This last feature is not inconsistent with the finding of a binding commercial relationship, as it is common to conceive agreements where one or more parties have the right to withdraw at any time.[128]

In conclusion, in Europe data protection enjoys the status of a fundamental right.[129] This qualification does not entail a prohibition to trade and economically exploit personal data; however, given that data protection is rooted in the context of personality rights, personal data cannot be considered a mere commodity, and the scope of negotiation is subject to some restrictions, aimed at avoiding the risks of violation of the personal sphere.[130] The GDPR sits within this framework and, as it will be better examined below, introduces a specific regime conceived for the peculiar interests involved, under which the use (so called "processing"[131]) of personal data can take place.[132]

4. Personal data as a counter-performance: a GDPR analysis

As described in Paragraph 2, personal data have an economic value and are often

of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC [2014] OJ L158/1 states that «no incentives or financial inducements are given» to «incapacitated participants», «minors» or «pregnant women». Also, Article 28, in general, states that «no undue influence, including that of a financial nature, is exerted on subjects to participate in the clinical trial». Certain EU Member States prohibit compensation *tout court* (for instance Italy, Legislative Decree 24 June 2003, no. 211, Article 1), others require the involvement of an ethics committee.

[124] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 58.

[125] H. Zech, *Data as a tradeable commodity* in A. De Franceschi (ed.), *European contract law and the Digital Single Market*, Cambridge, 2016, 51 ss., spec. 67.

[126] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 61-64, argues that this derives from the fact that the economic and non-economic aspects of personality are deeply connected.

[127] As to the processing personal data see Article 7(3) GDPR.

[128] S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 102-104.

[129] P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 49; N. Purtova, *Private Law Solutions in European Data Protection*, cit., 181.

[130] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 39.

[131] Article 4(2) GDPR.

[132] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 62.

exchanged for digital services/content, or for incentives, such as discounts or remuneration. Thus, personal data are considered as a de facto "price", "consideration" or "counter-performance" within a contractual relationship.[133] This reality has been taken into account by the EU legislation concerning consumer rights.[134] For instance, as mentioned in Paragraph 1 above, the Directive 2019/770 and the Directive 2019/2161 expand the protection for consumers to online contracts supplying digital services and digital content which are not paid with money, but for which consumers provide personal data[135], therefore acknowledging "payment" with personal data. While the in-depth analysis of these legal instruments is out of the scope of this paper, it is interesting to note that the language of the Directives changed compared to the initial proposals, as all references to the concept of providing personal data as a "counter-performance" have been removed and it is now specified that data protection is a fundamental right and «personal data cannot be considered as a commodity».[136]

This change reflects the dichotomy between data protection law, which restricts data collection and the possibility of tying the access to a service on the provision of consent to the processing of personal data, and consumer law, which otherwise tends to recognize the above consent as a counter-performance and to protect the transparency of market transactions. It is this ambivalence that has been noted by the EDPS which, in its opinions has expressed profound doubts on the concept of personal data as a counter-performance[137] and on whether individuals can "pay" with their personal data.[138] Overall, these opinions are not fully convincing. The reasoning for recommending the linguistic change is based on two main arguments: one is that data protection is a fundamental right and cannot be reduced to a "mere economic asset"[139], and the other regards the difficulties for individuals in understanding the value of their personal data.[140] However, it has already been argued that the first reason is not absolute and trenchant (see Paragraph 3), and the second issue could be solved by strengthening/introducing transparency rules (see Paragraph 2).

Moreover, the EDPS' concern – this instead being understandable - is to avoid the idea that personal data could always be processed with no limits when they are considered a counter-performance in an agreement.[141] On the contrary, the GDPR shall always be taken into account for the use of personal data in the digital economy.[142] Indeed, while the data protection law substantially regulates the personal data market, establishing if

133 G. Malgieri, *Data Extra Commercium*, cit., 7.

134 *Ibid.*

135 European Commission, *A New Deal for Consumers: Commission strengthens EU consumer rights and enforcement*, 11 April 2018.

136 Directive 2019/770, Recital 24.

137 EDPS 2017, cit.; EDPS, *Opinion 8/2018 on the legislative package "A New Deal for Consumers*, 5 October 2018 ("EDPS 2018").

138 EDPS 2018, cit., 3.

139 EDPS 2017, cit., 7; EDPS 2018, cit., 13.

140 EDPS 2017, cit., 9-10; EDPS 2018, cit., 13.

141 EDPS 2017, cit., 13.

142 EDPS 2018, cit., 12; EDPS 2017, cit., 3.

and when the exchange of personal data is allowed, consumer law regulates the modalities of such exchange, guaranteeing its transparency, regardless of its lawfulness. In other words, consumer protection instruments do not seem to be equipped to indicate whether it is lawful to exchange personal data on the market, but only indicate how such an exchange should be conducted. Therefore, in order to understand whether or not an exchange of personal data understood as a contractual counter-performance is lawful, it is necessary to have regard not to consumer law, but to data protection regulations and in particular, the GDPR.[143]

Thus, turning to the GDPR, this does not explicitly deal with trade and monetization of personal data; indeed, the difficulty in such situations is identifying a suitable legal basis, capable of guaranteeing the balance between the adequate protection of persons and the free flow of personal data.[144] This section will analyze the legal basis of contract (Article 6(1)(b) GDPR) and consent (Article 6(1)(a) GDPR) to examine whether they allow personal data to be exchanged as a counter-performance. To consider personal data as a counter-performance means to identify a synallagmatic/bilateral exchange between the user's personal data and the provider's service and thus to consider the processing of personal data as a condition to access the service.[145]

According to Article 6(1)(b) GDPR, personal data may be processed if "necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". The main issue is to assess the meaning of "necessary". According to the EDPB, the concept of "necessary" is to be interpreted strictly, as referring exclusively to those personal data that are "genuinely necessary" for the performance of the contract.[146] The following factors can be taken into account to assess when this is the case: (i) the «nature of the service being provided»[147] and the «distinguishing characteristics»[148]; (ii) the «rationale of the contract (i.e., its substance and fundamental object)»[149] and (iii) the «mutual perspectives and expectations of the parties to the contract»[150]; how the service is promoted or advertised.

That said, as mentioned, certain business models consider the processing of personal data as an alternative to a monetary payment in a contract, thus personal data are often compared to money ("payment" with personal data). In such cases, one could argue that personal data are indeed necessary for performing the contract, similarly as

143 S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *questa Rivista*, 3, 2019, 131 ss.

144 Garante per la protezione dei dati personali, *Relazione annuale 2019*, cit., 124-125.

145 S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., 181.

146 Article 29 Working Party ("WP29"), *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014; EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 8 October 2019.

147 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 10.

148 *Ibid.*

149 *Ibid.*

150 *Ibid.*

credit card details are necessary when a user decides to pay by credit card on an online website.[151] However, this view is strongly opposed by the EDPS as there is a risk of commodifying personal data.[152] While it is agreed that the analogy between personal data and money should be avoided (as mentioned in Paragraph 3 personal data are not fully commodifiable), the notion of "necessity" should be interpreted on a case-by-case basis. Depending on the nature of the service there may be different situations where it is arguable that the processing is necessary for the performance of a contract. For instance, a user of an online retailer may expect that among the «distinguishing characteristics»[153] of that service is the personalization of content[154], also in light of the fact that it is promoted as an «intrinsic element»[155] of such online service. Therefore, in that case it could be arguable that the processing of personal data for such purpose is necessary for performing the contract.[156] Moreover, Article 6(1)(b) GDPR - subject to a case-by-case analysis - could be a suitable legal basis for data processing in personal data economy models. In these situations, it is arguable that the substance of the agreements[157] usually coincides with carrying out online behavioural advertising or marketing to extract value from individual's personal data. Therefore, the processing of personal data for such purposes could be considered necessary for performing the agreement.[158] Again, the EDPB's opinion on this is strict: it is advanced that the processing of personal data for online behavioural advertising is *normally* not necessary for the performance of a contract and this conclusion is supported by the existence of the absolute right to object to direct marketing, including the related profiling, under Article 21 GDPR.[159] One could think that the EDPB's concern is that the contractual legal basis could entail the waiver of right to object under Article 21 GDPR – which would not be lawful. However, in the writers' opinion, the right to object under Article 21 GDPR could still be granted and enforced at any time; the exercise of such right would simply lead to the termination of the contract, which in fact could not be performed without the data processing opposed by the individual.

Finally, a further interpretation of the concept of "necessity" could be developed. It could be argued that the processing of personal data may be based on Article 6(1)(b)

151 WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, cit., 16.

152 EDPS 2018, cit., 14.

153 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 10.

154 Such as the recommendation of products users might like.

155 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 10.

156 However, see EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 16, whose opinion is very strict.

157 29WP, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, cig., 17 referring to the importance «to determine the exact rationale of the contract…, as it is against this that it will be tested whether the data processing is necessary for its performance».

158 This situation is different from the one described by 29WP (n 137) 17.

159 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 14-15.

GDPR when it is "financially necessary" to perform a contract (for example, a "free" social network collects personal data for online behavioural advertising to fund its service). However, the EDPB's opinion is that the processing of personal data which supports the provision of a service is «*in itself* not sufficient to establish that it is necessary for the performance of the contract».[160] Therefore, for the time being, a "financial necessity" concept is still unsupported and the provider's business model is only one of the factors to consider for a data processing to be necessary, together with the others listed above. Nevertheless, if a hypothetical data processing is found "financially necessary" to perform a contract, the data processing would still need to comply with the GDPR general principles, such as fairness and transparency, purpose limitation and minimization principles.[161] Also, ideally, strict transparency obligations should be introduced; for instance, the data controller – in compliance with the accountability principle[162] - would need to adequately reason the "financial necessity", explaining that although the requested service can be provided without that specific processing (i.e., objective necessity[163]), it cannot be financially supported; moreover, it would need to disclose the methods to evaluate personal data, the value of personal data and the amount and type of personal data necessary to support that service and thus perform the contract.

As to the legal ground of consent under Article 6(1)(a) GDPR, this shall be free and revocable.[164] Consent is freely given if individuals have «real choice and control»[165] on the use of their personal data and may refuse consent without detriment and withdraw consent easily at any time.[166] Article 7(4) GDPR specifies that «when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract». Also, Recital 43 GDPR provides that: «Consent is presumed not to be freely given […] if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance».

In other words, there is a presumption that consent to data processing is not freely given - and thus is invalid - when it is a condition for the provision of a service (i.e., consent to data processing as a counter-performance in an agreement).[167] Article 7(4) GDPR has been the object of an intense debate regarding its interpretation. On one side, scholars argue that this provision does not introduce a ban on the possibility to establish a link between the provision of the service and consent to data processing

[160] Ivi, 15.

[161] Articles 5.1.a-c GDPR.

[162] Article 5.2 GDPR.

[163] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 9.

[164] Recitals 32, 42, 43, Articles 4(11), 7 GDPR.

[165] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020.

[166] Recital 42; Article 7(3) GDPR.

[167] G. Malgieri, *Data Extra Commercium*, cit., 7.

and argue for a flexible approach[168], on the other, the EDPB[169] and certain DPA's[170] have a stricter view and observe that «there might be very limited space for cases where this conditionality would not render the consent invalid»[171] and it is likely unusual to rebut the presumption that «bundled consent is not freely given».[172] Clearly, adopting one view or the other affects the extent to which personal data can be commercialized and monetized on the basis of consent.

A careful reading of the EDPB's opinion on Article 7(4) GDPR[173] brings to the following considerations. The EDPB's explicit statement that consent to data processing «cannot become directly or indirectly the counter-performance of a contract»[174] should be interpreted in the sense that consent to the unnecessary processing of personal data cannot be construed always and in any circumstances as «a mandatory consideration in exchange for the provision of a service».[175] However, consent to data processing can be incentivized and still be considered free.[176] Thus, the issue is to distinguish between a non-permissible and a permissible incentive, which would allow individuals to obtain "free" services, or a discount or remuneration, in exchange of their personal data.

The following factors may be considered to assess the freedom of consent: (i) whether there is a «genuine choice»[177] between a service that requires consenting to personal data processing for additional purposes and an «equivalent service»[178] which does not require such consent; (ii) whether those who do not give or withdraw their consent are «unfairly penalized»[179]; (iii) an imbalance of powers between individuals and the data controller[180]; and (iv) the level of transparency of data processing.[181]

As to (i), a genuine choice should concern a "genuinely equivalent service" offered by the same data controller (alternatives offered by third parties on the market are irrelevant[182]). It is arguable that a paid service with no collection of personal data for additional purposes is a genuine alternative to a "free" service with the users' bundled

168 G. Resta – V. Zeno-Zenovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile* 2, 2018, 411 ss., spec. 430; A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *JIPITEC*, 8, 2017, 5 ss.; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 96; G. Malgieri, *Data Extra Commercium*, cit., 8.

169 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit.

170 Information Commissioner's Office ("ICO"), *Consent*, 22 March 2018.

171 EDPB, cit., 10.

172 ICO, cit., 10.

173 EDPB, cit.

174 Ivi, 9.

175 *Ibid.*

176 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 12.

177 Ivi, 10.

178 *Ibid.*

179 ICO, *Consent*, cit., 24.

180 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 7-8.

181 Ivi, 14-16.

182 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 10.

consent to additional data processing[183] (for example, a fee to use the wi-fi at the airport with no collection of unnecessary personal data versus a "free" wi-fi at the airport with personal data processing for marketing).[184] The argument that a paid service is a genuine alternative to a "free" service is also supported by the fact that the Article 29 Working Party's revised guidelines on consent do not include anymore the specification that the equivalent service shall not include "further costs".[185] Also, it seems permissible that an online retailer offers a certain discount only to the users that consent to receiving a newsletter, while those who do not want to give their consent would only be able to access the retailer's website and receive general discounts during the end-of-season sale. As to (ii), the refusal or withdrawal of consent should be without detriment[186], that is with no disadvantages[187]. If a user chooses to "pay" with data instead of money and then withdraws her consent, the consequence would be the denial of the "free" service, while the paid alternative would still be available[188]; this however does not amount to a disadvantage, as the loss of a permissible incentive does not entail a detriment for the individual.[189] Moreover, an imbalance of powers (point iii) may occur in situations where (a) there are negative consequences if the individual does not consent, such as "substantial extra costs"[190], or (b) if «there is an element of compulsion, pressure or inability to exercise free will».[191] A reasonable fee or the loss of a discount do not seem to imply "substantial extra costs".[192] Also, arguably the request of a bundled consent in certain contexts, such as by an online retailer or in a recreational context[193], does not imply a negative pressure on the user. On the contrary, it would not be permissible for a health care provider to offer "free" health care only to individuals consenting to targeted advertising, and, as an alternative, a paid health care service to those who do no consent to additional data processing. Indeed, individuals suffering of health issues are in a position of vulnerability and could feel a negative pressure to consent to unnecessary data processing to gain access to free health care.[194] Thus, the nature of the service should also be taken into account: when the service provided in exchange for

183 G. Malgieri, *Data Extra Commercium*, cit. 8.

184 The fee must be "reasonable": in line with the market rates applied in similar cases (e.g. hotels or other accommodation facilities), so that the option to use the wi-fi with monetary payment is an effective alternative and not only a theoretical one.

185 29WP, *Guidelines on Consent under Regulation 2016/679*, 28 November 2017.

186 Recital 42 GDPR.

187 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 11, 22 refers to «lowering the service level».

188 According to S. Thobani (*Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 188) this derives from the fact that consent to data processing is the counter-performance to access the service.

189 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 12.

190 Ivi, 8.

191 *Ibid.*: in relationships with public authorities or employers.

192 D. Zetoony, *Does the GDPR prohibit charging more to consumers that do not consent to certain types of processing?*, in *bclplaw.com*, 8 June 2020.

193 A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, cit., 5.

194 29WP, *Opinion 15/2011 on the definition of consent,* WP187, 13 July 2011.

consent to data processing is essential[195] and of particular importance for an individual, consent to data processing could be unduly conditioned.[196] Finally (point iv), not only individuals should receive a clear information notice on the use of their personal data, but also an explanation of the commercial nature of the transaction, where personal data represent the counter-performance in the agreement[197], the consequences of consenting or withdrawing such consent, and the value of their personal data.[198]

That said, different approaches have been adopted regarding the notion of free consent and the interpretation of Article 7(4) GDPR. For instance, the Italian DPA has been consistent in the strict interpretation of free consent in the sense that consent is not free where access to a good or service is subject to giving consent[199]. For instance, recently, it found unlawful to require individuals to give their consent to marketing activities in order to gain access to certain discounts and to enter prize competitions[200]; as to the ICO, it is noteworthy to refer to a case where it warned the Washington Post that its online practice did not comply with the GDPR. More specifically, the Washington Post required its users to choose between (a) consenting to cookies in order to obtain "free" access to a limited amount of articles; (b) paying a basic subscription fee, plus consenting to cookies in order to access to an unlimited number of articles; or (c) paying a higher subscription fee without the need to consent to personal data collection through cookies in order to access to an unlimited number of articles. This consent was not considered freely given as there was no «*free* alternative to accepting cookies on its website» and the Washington Post should ensure access to all levels of subscription without users having to consent to the use of cookies.[201] On the contrary, in a similar case where access to an online newspaper was conditional on consenting to the use of cookies, the Austrian DPA found that consent was freely given as individuals «did not face significant negative consequences since they could choose to subscribe to the site for a small fee or simply choose another online newspaper as a source of information».[202] Finally, an interesting view has been expressed by the Italian Supreme Court[203] which clearly affirmed that the «exchange of personal data»[204] is not

195 S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 167 referring to remuneration in an employment relationship, banking, financial and health services.

196 *Ibid.*

197 This work is focused only on data protection; however, transparency and fairness should be guaranteed also through the application of the consumer protection legislation (see for example note 52).

198 G. Malgieri, *Data Extra Commercium*, cit., 14-16.

199 For instance, see Italian DPA, Decision no. 2542348, 4 July 2013, according to which «the consent given is not free when the company conditions the registration to its website and, consequently, also the access to its services, to the user's consent to the processing of personal data for promotional purposes».

200 Italian DPA, Decision no. 9256486, 15 January 2020.

201 ICO, Case Reference Number: RFA0768934, 11 October 2018.

202 H. Andrews Kurth LLP, *Austrian DPA Issues Decision on Validity of Cookie Consent Solution*, in *lexology.com*, 7 January 2019; *Datenschutzbehörde* (Austrian DPA), "*Bescheid vom* 30.11.2018, GZ: DSB-D122.931/0003-DSB/2018", 30 November 2018, accessed 30 July 2020.

203 Cass. civ. 2 July 2018, no. 17278, in *Guida al diritto,* 2018, 31, 20.

204 *Ibid.*

prohibited as long as it is «the result of consent which is not coerced»[205]; in this specific case, it found permissible to subject access to a service to consent to unnecessary data processing, provided that such a service is "fungible", i.e., similar alternatives are available on the market, and not "indispensable", that is non-essential for the individual.[206] Following this reasoning, as money is by definition fungible, it should be permissible to offer remuneration in exchange of personal data, as individuals who do not want to give their consent to personal data processing could find alternative ways to obtain remuneration.[207]

In conclusion, strictly speaking, some of these positions do not follow the EDPB's opinion in full[208]; in fact, the ICO refers to the necessity that the genuine alternative is also "free" - while this condition has been removed by the EDPB; and the Austrian DPA and Italian Supreme Court to the existence of alternatives offered by third parties - while the EDPB refers only to the alternatives offered by the same data controller.

Notwithstanding the lack of uniformity, it could be arguable that the GDPR does not prohibit the commercial exchange and monetization of personal data. However, the general limit to creating a link between the performance of a contract/provision of a service and the processing of personal data as a counter-performance is to not unduly condition individuals.

5. Conclusion

Personal data-centered business models are a clear index of the economic value of personal data and that these are being traded and monetized on the market. This paper has acknowledged the benefits and downsides of these businesses and reasoned on the lawfulness of such practices. The possibility to exchange personal data in return for products/services or other incentives (i.e., personal data as a counter-performance in an agreement) depends on the approach to the right to data protection. In Europe, the right to data protection is a fundamental right and a personality right. Thus, there is a tension between the protection of personal data as intangible aspects of a person's identity – our digital soul – which argues for the inalienability of personal data - and the exploitation of their economic value. This tension can be solved by considering that (i) the fundamental right to data protection is not absolute and shall be balanced with the freedom to conduct a business and to contract and the free flow of personal data and that (ii) intangible aspects of personality rights can indeed be traded with the limit of their non complete alienation. This paper then assesses the specific rules governing personal data processing. It analyses the GDPR legal bases of contract (Article 6(1)(b)) and consent (Article 6(1)(a)) as possible grounds to justify the tradability of personal data. Given the current rigid interpretation of the lawful basis for contracts,

205 *Ibid.*

206 *Ibid.,* the service consisted in an online newsletter.

207 S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali,* cit., 168.

208 It is noted that these opinions are not binding.

the legal ground of consent seems to be preferable. This work concludes that, while it is discouraged to ask individuals to provide their personal data in exchange for an advantage or as an alternative to money, there is room to interpret the legal basis under Article 6(1)(a) GDPR (consent) in ways that could allow the commercialization and monetization of personal data if that consent is "freely" given,[209] depending on a case-by-case analysis. In essence, individuals should be given a genuine choice between a service that is conditional on consent to personal data processing for additional purposes and an equivalent service that does not require such consent. Also, the service concerned should not be essential, as individuals would be unduly conditioned. Finally, individuals should be able to choose consciously by clearly understanding the nature, the convenience, and the consequences of these type of agreements. This last aspect requires the enforcement of existing transparency rules and the introduction of new ones. Following this approach, there might be business models offering product/service differentiation based on users' privacy preferences[210] and many more offering personal data remuneration. It would then be left to service providers to conceive solutions which are more attractive for users so to lawfully incentive them to provide their personal data[211] and to data protection authorities to supervise these and prevent risks to individuals' dignity and personality.[212]

[209] G. Malgieri, *Data Extra Commercium*, cit., 8.

[210] R. Auf Der Maur – D. Fehr-Bosshard, *Data Monetization and User Consent: better privacy or more bureaucracy?*, in *vischer.com,* 6 September 2017, 247.

[211] Ivi, 248.

[212] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 433-434.