German Law Journal (2020), **21**, pp. 924–943
doi:10.1017/glj.2020.47

CAMBRIDGE UNIVERSITY PRESS

ESSAY

Commerce in Data and the Dynamically Limited Alienability Rule

Václav Janeček* and Gianclaudio Malgieri**

(Received 09 July 2019; revised 11 September 2019; accepted 08 October 2019)

Abstract

Commerce in some data is, and should be, limited by the law because some data embody values and interests—in particular, human dignity—that may be detrimentally affected by trade. In this Article, drawing on the Roman law principles regarding *res extra commercium*, we investigate the example of personal data as regulated under the EU Charter and the GDPR. We observe that transactions in personal data are not forbidden but subject to what we call a dynamically limited alienability rule. This rule is based on two dynamic variables: The nature of data and the legal basis for commercially trading such data at a primary or secondary level. Accordingly, in order to deal with such dynamism and the uncertainty it poses, we propose a general two-stage reasonableness test that should help legal practitioners, judges, and lawmakers to consider when trade in data is illicit and who, if anyone, shall be held responsible for this mischief. Finally, we show how the two-stage test and the limited alienability rule can advance European contract law and help enforce legal principles associated with such *data extra commercium* in automated and autonomous data trading systems.

Keywords: Alienability; contract law; data; data commerce; digital assets; Digital Single Market; GDPR; inalienability; ownership; personal data; *res extra commercium*; sensitive data; trade

A. Introduction

Law permits trade in data, so it seems that data are alienable objects (*res in commercio*).[1] In this Article, we argue that commerce in some data is, and should be, prohibited by the law because some data embody values and interests that would be detrimentally affected by trade. We survey

*Václav Janeček is a DPhil in Law candidate and Research and Course Development Fellow in Law and Technology at the Faculty of Law, University of Oxford.

**Gianclaudio Malgieri is a Doctoral Researcher in the Law, Science, Technology, and Society (LSTS) Research Group at the Vrije Universiteit Brussels and an incoming Associate Professor at EDHEC Business School.

Both authors would like to thank the organizers of the 5th Münster Colloquia on EU Law and the Digital Economy, the TILTing Perspectives 2019, and the Oxford EU Law Discussion Group for inviting us to present this Article, and to the participants in these events for their valuable feedback. Our thanks are also due to Jürgen Basedow, Kristin Boosfeld, Leah Grolman and the German Law Journal's anonymous referee for their comments. The usual disclaimer applies. Both authors contributed to this Article equally. The authors declare no potential conflict of interest.

This Article is based on a book chapter: Václav Janeček & Gianclaudio Malgieri, *Data Extra Commercium*, *in* DATA AS COUNTER-PERFORMANCE—CONTRACT LAW 2.0? (Sebastian Lohsse et al. eds., 2020).

[1]*See, e.g.*, Alberto De Franceschi, *European Contract Law and the Digital Single Market: Current Issues and New Perspectives*, *in* EUROPEAN CONTRACT LAW AND THE DIGITAL SINGLE MARKET: THE IMPLICATIONS OF THE DIGITAL REVOLUTION 5 (Albert De Franceschi ed., 2016) ("In the digital world, data are in fact an important '*res intra commercium*,' namely tradeable good.").

the legal limits on trading data in the digital economy and ask whether, and to what extent, a set of principles can rationalize (1) when data qualify as *extra commercium* and (2) who is to be held responsible for the illicit trade in the *data extra commercium*. By answering these two questions, we fill an important gap in the existing legal scholarship.

The problem is that, unlike in the case of traditional goods (*res*), inalienability of data cannot be ascertained *ex ante* because the question of whether or not a particular dataset represents values and interests that can be compromised by commerce is not a question about a static property of the dataset. We argue that alienability of data, unlike alienability of traditional goods, is limited by dynamic changes that have direct implications for data alienability. According to our research, these changes take place at the level of informational properties of data, such as when data are processed in a new context by a new analytic algorithm, and at the level of legal bases for trading data, such as when a data subject withdraws her consent in relation to processing of personal data.[2] This means, among other things, that alienability of data can be limited even *ex post*. Along these lines, by analyzing the legal framework around personal and sensitive data protection, we develop a "dynamically limited alienability rule" that concisely describes the principles of inalienability of personal and sensitive data under the GDPR.

This Article is structured as follows: Section B introduces the Roman law doctrine of *res extra commercium* and shows why it is inspiring in relation to trade in data. While the doctrine cannot account for the fluid nature of data nor the technology-driven virtual environment in which data are processed and traded, the infosphere,[3] the rationales for excluding some data from trade do not change and have legal implications very similar to the rationales behind *res extra commercium*. Accordingly, responsibility for trade in *data extra commercium* can be attributed almost fully in line with the principles behind the Roman law doctrine. Section C surveys positive law. We observe that no legal provision expressly addresses the question of (in)alienability of data, although data protection laws clearly seem to protect human flourishing. One thus cannot easily ascertain whether and when trade in data is illicit due to those data being qualified as *extra commercium*. We fill this gap by identifying and compiling legal rules that limit alienability of data, namely personal and sensitive data. To help advance EU law and transnational data trade while ensuring protection of the fundamental values that the law excludes from trade, we formulate what we call a "dynamically limited alienability rule". In Section D, we seek to help legal practitioners, judges, and lawmakers to consider who, if anyone, shall be held responsible and eventually also liable for this mischief. Building on Roman law and modern contract law principles, we thus propose a general two-stage test that satisfies our goal. In Section E, we discuss how the two-stage test and the limited alienability rule may help link the EU data protection law with contract law rules and principles, and help enforce legal principles of *data extra commercium* in fully automated and autonomous data trading systems which are becoming increasingly significant for our daily lives.

Overall, our main original claims are that data are subject to a dynamically limited alienability rule and that responsibility for the consequences of inalienability of data can be determined using the two-stage test that we propose. We argue that *data extra commercium* is a useful dynamic concept that helps protect certain values and interests in the infosphere and can be employed in traditional European contract law.

For reasons set out below, we focus primarily on trade regarding personal data and other sensitive data. For reasons also set out below, we restrict this Article to questions of when and how we should protect these data. In contrast, we do not look at how we should protect parties

[2]Regulation (EU) 2016/679, Article 7(3), 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/EEC, 2016 O.J. (L 119) 1 [hereinafter GDPR].

[3]*See* Luciano Floridi, *Technology's In-Betweeness*, 26 PHIL. AND TECH. 111 (2013); LUCIANO FLORIDI, THE FOURTH REVOLUTION: HOW THE INFOSPHERE IS RESHAPING HUMAN REALITY ch. 2 (2014).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

if their contract is negatively affected by data protection tools. That is, we do not look at what remedies should be available to them. In addition, when we discuss attribution of responsibility, we do not mean to say that the law imposes a duty on a party to observe certain rules with respect to data or that the law imposes liability on a party for failing to respect certain rules. These issues would need to be resolved at the level of national legal systems, which is beyond the scope of this Article. What we mean instead is that national legal solutions should adhere to the principles we describe.

B. From *Res Extra Commercium* to *Data Extra Commercium*

The Roman law protected multiple types of thing (*res*) by excluding them from commerce (*extra commercium*). The commercial inalienability of these things was entrenched in the values and interests that *res extra commercium* embodied. Accordingly, Roman law prohibited trade in free humans (*liberi homines*),[4] things of divine interest (*res divini iuris*),[5] and things of secular public interest (*res publicae*).[6] Although we no longer use the Roman law doctrine of *res extra commercium*, these categories evoke some strong parallels with the recent prohibitions regarding human trafficking,[7] trade in human organs,[8] trade in some religious and cultural artifacts,[9] unlicensed commerce in publicly dangerous or invaluable things,[10] and traffic in publicly important things which are either considered common to everyone or that belong to no one.[11]

A purported sale of any of these three categories of thing was first deemed void as legally impossible,[12] except where the purchaser, without fault on his part, was unaware of their real nature.[13] The tendency to protect the buyer is understandable as "it can be difficult to distinguish a free man from a slave".[14] It is also understandable to have regard to the buyer's fault, because "even the greenest provincial on his first visit to the mother city could [not] honestly believe that he could take effective possession [. . .] of, say, the Temple of Venus or the *Porta Capena* or, turning to *res publicae*, of the Theatre of Pompey or the *Via Sacra*".[15]

[4]Dig. 18.1.4 (Pomponius, Ad Sabinus 9); Dig. 18.1.6pr. (Pomponius, Ad Sabinus 9); Dig. 18.1.5 (Paul, Ad Sabinus 5); Dig. 18.1.34.2 (Paul, Ad Edictum 33); Dig. 18.1.70 (Licinius, Regulae 8); J. Inst. 3.23.5.

[5]*See* J. Inst. 2.1.7–10; J. Inst. 3.23.5; G. Inst. 2.5–6; Dig. 11.7.8.1 (Ulpian, Ad Edictum 25); Dig. 18.1.4 (Pomponius, Ad Sabinus 9); Dig. 18.1.22 (Ulpian, Ad Sabinus 28); Dig. 18.1.23 (Paul, Ad Sabinus 5); Dig. 18.1.62.1 (Modestinus, Regulae 5). *See also* John Baron Moyle, The Contract of Sale in the Civil Law 19 (1892); Joseph Anthony Charles Thomas, *The Sale of Res Extra Commercium*, 29 Current Legal Problems 136, 137 (1976); Robin Evans-Jones & Geoffrey MacCormack, *The Sale of Res Extra Commercium in Roman Law*, 112 Zeitschrift der Savigny-Stiftung für Rechtsgeschichte (rom. Abt.) 330, 342 (1995);.

[6]Dig. 18.1.35.2 (Gaius, Ad Edictum Provincia 10); Dig. 18.1.52 (Paul, Ad Edictum 54); Dig. 39.2.48 (Marcian, Delatores). *See also* Thomas, *supra* note 5, at 138.

[7]*E.g.*, United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children of 2000, supplementing the United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2337 U.N.T.S. 319.

[8]*E.g.*, Council of Europe Convention Against Trafficking in Human Organs, Mar. 25, 2015, C.E.T.S. 216.

[9]*E.g.*, UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, Nov. 14, 1970.

[10]*E.g.*, Single Convention on Narcotic Drugs, Mar. 30, 1961, 976 U.N.T.S 105; Convention on International Trade in Endangered Species of Wild Fauna and Flora, Mar. 3, 1973, 993 U.N.T.S. 243 [hereinafter CITES]; Arms Trade Treaty, Dec. 24, 2014, 3013 U.N.T.S. 1.

[11]*E.g.*, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Oct. 10, 1967, 610 U.N.T.S. 205.

[12]Dig. 18.1.34.1 (Paul, Ad Edictum 33) ("[. . .] earum nulla venditio est.").

[13]Dig. 19.1.4pr. (Paul, Ad Sabinus 5). *See also* Moyle, *supra* note 5, at 19; Thomas, *supra* note 5, at 138–39.

[14]Dig. 18.1.5 (Paul, Ad Sabinus 5) ("Quia difficile dinosci potest liber homo a servo."). *See also* Ernest Metzger, *Remarks on David Daube's Lectures on Sale, with Special Attention to the* liber homo *and* res extra commercium, *in* David Daube: A Centenary Celebration (Ernest Metzger ed., 2010).

[15]Thomas, *supra* note 5, at 139.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

Eventually, the various rules have been compiled into a specific provision of Justinian's *Institutes* (Inst.III.23.5), according to which a person who, in full awareness of the facts, bought a thing in which trade is forbidden, bought in vain and his contract was void. Yet if the purchase was based on the seller's fraud, deception, or misrepresentation,[16] the law granted the buyer a remedy in damages for mischiefs such as eviction, confiscation, and misapprehension induced by the seller. To the extent that these remedies were conditioned on a breach of contract, the jurists felt that they should not to deem the contract void because otherwise there would be no legal basis for the remedy. This required an exception to be made to the general rule that fraud renders a contract void *ab initio*.[17]

Recent EU laws and other legal rules also protect certain types of valuable assets by excluding them from commerce. We focus on data. The laws regarding data and digital content seem to exclude some data types from commerce, although somewhat ambiguously, as we will show in Section C. Thus, it effectively looks as if some types of data—due to characteristics of the information they embody—cannot be the subject of a sale contract (*extra commercium*), similarly to how Roman law prohibited trade in certain types of thing. Yet as we have seen in the introduction, trade in data, unlike trade in material objects, poses some very challenging questions. In particular, it seems that we need to think dynamically about the values and interests that the data represent, and it is unclear what implications this may have for the validity of contracts and the availability of contractual remedies in relation to *data extra commercium*. Let us investigate these issues in relation to personal data.

The parallels between *res extra commercium* and our proposed concept of *data extra commercium* look particularly strong in the case of free humans and personal data. Illicit trade in free humans, unlike trade in things of divine or public interest, was allegedly an increasingly common source of practical trouble in Roman times.[18] An analogy may be drawn with recent illicit handling of personal data by tech giants such as Facebook.[19] Also, in Roman times, free individuals were not "things" in a legal sense, just as data are not considered to be "things" in many modern jurisdictions.[20] Finally, the distinction between a slave and a free individual is epistemically obscure, just as there is no clear line between non-personal and personal data.[21] Both a slave and a free individual are humans, although they embodied different values in Roman law. Both non-personal and personal data are data, although they encapsulate different types of valuable information.

Given that the distinction between a free individual and a slave is no longer legally significant, we could instead seek to draw an analogy with trade in human organs. Although organs are different from data—and, generally, from intangible goods—legal protection of human organs has been widely compared with legal protection of personal data.[22] This is perhaps due to the central role of

[16]Innocent deception incurred milder redress. *Cf* Thomas, *supra* note 5, at 138; DIG. 18.1.45 (Marcian, Regulae 4); DIG. 19.1.13pr.–4 (Ulpian, Ad Edictum 33).

[17]Evans-Jones & MacCormack, *supra* note 5, at 350.

[18]Evans-Jones & MacCormack, *supra* note 5, at 331.

[19]*E.g.*, Landgericht Berlin [LG] [Regional Court] Jan. 16, 2018, 16 O 341/15 (Ger.).

[20]*Cf., e.g.*, BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], § 90, *translation at* http://www.gesetz-im-internet.de/englisch_bgb/index.html (Ger.) ("Sachen im Sinne des Gesetzes sind nur körperliche Gegenstände." ("Things in legal sense are only physical objects.")). *See also* Codice civile [C.c.] [Civil Code], Article 810, 814 (It.); Andreas Boerding et al., *Data Ownership—A Property Rights Approach from a European Perspective*, 11 J. CIV. L. STUD. 323, 336–38 (2018).

[21]*See* Sophie Stalla-Bourdillon & Alison Knight, *Anonymous Data v. Personal Data-False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, 34 WIS. INT'L L.J. 284 (2016); Christiane Wendehorst, *Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy*, *in* TRADING DATA IN THE DIGITAL ECONOMY: LEGAL CONCEPTS AND TOOLS 332 (Sebastian Lohsse et al. eds., 2017); Václav Janeček, *Ownership of Personal Data in the Internet of Things*, 2018 COMPUTER L. & SEC. REV. 1039, 1042–44 (2018).

[22]*See* Stefano Rodotà, *Trasformazioni del corpo*, 37 POLITICA DEL DIRITTO 3 (2006); Giusella Finocchiaro, *Corpo digitale e informazioni nella sanità elettronica*, 16 SALUTE E SOCIETÀ 32 (2017); Gianclaudio Malgieri, *R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions*, *in* DATA PROTECTION AND PRIVACY: THE INTERNET OF BODIES (Ronald Leenes et al. eds., 2018).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

personal data in constructing personal identity and to the inherently personal nature of both organs and data as components of the moral and physical integrity of human beings.[23] Accordingly, if the human body and its components are capable of being considered *res extra commercium*, one might be tempted to conclude that personal data—that is data that already relate to an identifiable human, just like organs pertain to an individual—are likewise inalienable in the European digital market.

Indeed, the rationales for excluding trade in human organs can partly translate to commerce in personal data—as we will see in the next two sections of this Article—but arguments about tradability of data must take a very different form. This is so because non-personal data can become personal, and vice versa. The difficulty with all data, not just personal data, is that one must always first compute the information that data embody in order to find out the legal status of such data. Data as objects of digital transactions can therefore never be excluded from commerce *ex ante*, because they can be *ex post* linked with values and interests that would be compromised by sale.

The dynamic nature of data is unparalleled in the physical world. The closest we could perhaps get is the example of 3D-printed organs.[24] Unlike organs extracted from a human, organs printed on a 3D printer are a tradable commodity. In the physical world, it is relatively easy to understand why the law prohibits trade in human organs but not trade in 3D-printed organs. The rationale for this protection seems to be based on moral and ethical considerations, grounded on human dignity in terms of moral and physical integrity.[25] For the same reasons, one could argue that it would be illicit to trade 3D-printed organs that have already been successfully implanted in a human body. While this looks like a dynamic change in the nature of those 3D-printed organs, however, it is important to highlight that this is a one-off change. In contrast, the nature of data may change repeatedly.

A further complication is that a data subject—that is a human to whom the personal data relate—may *ex post* withdraw her consent with processing of personal data for a specific purpose. Again, in the physical world, it would be hard to imagine that a producer of 3D-printed organs would terminate a contract and withdraw their organs from the human body. In the infosphere, however, a data subject can demand her data back, which causes some headaches for the contracts involving those data and attendant remedies.[26] We will get to these issues in Sections C, D and E.

For now, it suffices to highlight that these dynamic *ex post* changes in the nature of data are a new phenomenon that might lead to exclusion of data from trade. This issue seems to have slipped the attention of lawmakers as well as many scholars, although it presents a distinct problem for the data economy. As, for instance, Basedow argues, "[i]t should be clarified to what extent personal data are *res extra commercium* and what this means for contracts covering such data".[27] The uncertainty over when the law excludes data from commerce is further magnified by the fact that there are no clearly defined rationales for treating certain data as *res extra commercium* such as is

[23]*See* Rodotà, *supra* note 22.

[24]*E.g.*, Dina Radenkovic, Atefeh Solouk, & Alexander Seifalian, *Personalized Development of Human Organs Using 3D Printing Technology*, 87 MED. HYPOTHESES 30 (2016); European Commission Directorate-General for Research and Innovation, *Human Organ Replacement – Targeted scenario N°8* (2018) https://ec.europa.eu/info/sites/info/files/human-organ-replacement-targeted-scenario-8_2018_en.pdf.

[25]*See, e.g.*, Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, pmbl., Apr. 4, 1997, E.T.S. No. 164 ("Convinced of the need to respect the human being both as an individual and as a member of the human species and recognising the importance of ensuring the dignity of the human being.").

[26]*See* Stefan Grundmann & Philipp Hacker, *The Digital Dimension as a Challenge to European Contract Law—The Architecture*, *in* EUROPEAN CONTRACT LAW IN THE DIGITAL AGE 42–44 (Stefan Grundmann ed., 2018); Gerald Spindler, *Contracts for the Supply of Digital Content—The Proposal of the Commission for a Directive on Contracts for the Supply of Digital Content*, *in* EUROPEAN CONTRACT LAW IN THE DIGITAL AGE 285, 292, 306–07 (Stefan Grundmann ed., 2018).

[27]Jürgen Basedow, *The EU Digital Single Market Strategy and Insurance Law*, J. BUS. L. 455, 462 (2018) (discussing the contractual implications—termination, restitution, retroactiveness—of a consent withdrawal or a claim for erasure of personal data).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

the Roman law triad of reasons—an interest in liberty of free humans; a divine interest; and a public interest. Further, in cases of hidden data commodification and when data are provided instead of a monetary price for the provision of digital content, there is always an implicit danger that contracts involving such data would be invalidated *ex post*.

Thus, it seems worth attempting to map the concept of *data extra commercium* onto the moral and public policy reasons found in Roman law or a similar set of reasons, so as to clarify the constraints on trading data which are implicitly baked in our laws and provide a higher degree of certainty for the data economy. Due to the number of parallels and the reasons given, we will use personal data as a vehicle for our argument, although we aspire to make more general claims about limits on trade in data.

In this regard, Margaret Radin's work in which she challenges the idea of "paternalism" as a basis for market inalienability is particularly relevant.[28] By criticizing Calabresi and Melamed's famous view on inalienability,[29] Radin argues that the real justification of trade limitations should not be based on traditional liberalism or economics but on a conception of personhood and human flourishing. According to Radin, the reason why we do not trade children or human bodies is thus our interest in human flourishing. Human flourishing, a key concept in virtue ethics,[30] means the development and fulfilment of one's own personality, based on positive freedom (life, health, thought), negative freedom, and autonomy. Allowing individuals to trade their body parts or entire bodies, for instance, would impair the foundation of individuals' freedom, because it would be detrimental to personhood itself. Accordingly, inalienability should not be justified through paternalism but, on the contrary, through human freedom.

Radin was one of the first to discuss personal information in the context of the inalienability of human beings.[31] Indeed, she affirms that personal information—"attributes" and "characteristics"—is what makes personhood unique and, thus, it cannot be separated from persons themselves.[32] Following this line of argument, we can infer that if humans are inalienable, their personal data should likewise be inalienable, because only objects separate from the self are suitable for alienation. For example, the French national advisory Committee for Ethics, when interpreting Article 16-10 of the French Civil Code, considered the technology of genetic fingerprints (*empreintes génétiques*) as *res extra commercium*[33] because fingerprints are inseparably liked to an individual.

In other words, we think Radin's work identifies a strong rationale for what we call *data extra commercium*: Inalienability of personal information justified through arguments concerned with human flourishing. Interestingly, privacy scholars have recently affirmed that the right to human flourishing might be the general justification, or even the *raison d'être*, for the right to privacy as protected under Article 8 of the European Convention on Human Rights.[34] Overall, it seems that

[28]Margaret Radin, *Market Inalienability*, 100 HARV. L. REV. 1849, 1885 (1987).

[29]Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

[30]*See* Marta C. Nussbaum, *Capabilities and Human Rights*, 66 FORD. L. REV. 273, 297 (1997).

[31]Radin, *supra* note 28, at 1925, 1932 ("There is certainly the danger that women's attributes, such as height, eye color, race, intelligence, and athletic ability, will be monetized. Surrogates with 'better' qualities will command higher prices in virtue of those qualities. [. . .] When the baby becomes a commodity, all of its personal attributes—sex, eye color, predicted I.Q., predicted height, and the like—become commodified as well. This is to conceive of potentially all personal attributes in market rhetoric, not merely those of sexuality.") (footnote omitted).

[32]Radin, *supra* note 28, at 1885 ("Universal market rhetoric transforms our world of concrete persons, whose uniqueness and individuality is expressed in specific personal attributes, into a world of disembodied, fungible, attribute-less entities possessing a wealth of alienable, severable 'objects.' This rhetoric reduces the conception of a person to an abstract, fungible unit with no individuating characteristics.") (footnote omitted).

[33]ELS J. KINDT, PRIVACY AND DATA PROTECTION ISSUES OF BIOMETRIC APPLICATIONS: A COMPARATIVE LEGAL ANALYSIS 210 (2013). *See also* F. El Atmani, *Données sensibles: la notion de consentement de la personne concernée*, 86 LAMY DROIT DE L'INFORMATIQUE 1, 4 (1996).

[34]Bart Van der Sloot, *Privacy as Human Flourishing: Could a Shift Towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?*, 5 JIPITEC 230 (2014).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

inalienability of personal data could be justified on a moral basis, just like Roman law advanced moral reasons when prohibiting trade in free humans, because the morally-laden values and information that personal data embody would be compromised by sale. So, while the nature of data dynamically changes, the rationales for excluding some data from trade can remain unaltered. What dynamically changes is whether data encapsulate values and interests that would be detrimentally affected by trade, not whether we want to protect those values and interests. Building on the existing literature, we submit that human flourishing is regarded as one such fundamental value that can justify inalienability of personal data.

C. When the Law Limits Trade in Data?

The law is, however, not bound to follow such abstract moral arguments. It may build on them to provide a principled legal ground for excluding data from commerce, but it could just as easily disregard those rationales. Accordingly, the aim of this section is to explore whether, and under what conditions, there are already some forms of *data extra commercium* in EU law or in national legislation.

Before we begin, we stress that several leading commentators consider data to be *intra commercium* by default.[35] Indeed, Article 2(11) of the Directive on Consumer Rights seems to protect the commercial use of data in sales law by explicitly addressing production and supply of digital content.[36] The Regulation on a Framework for the Free Flow of Non-Personal Data[37] and the Digital Content and Digital Services Directive[38] support the same conclusion, as they consider data tradable goods. The Regulation, for instance, explicitly declares the objective of "removing obstacles to trade".[39] The Digital Content and Digital Services Directive, then, defines "digital content" as "data which are produced and supplied in digital forms"[40] and allows for data—even personal data—as an alternative payment for the supply of digital content and services.[41] Although the proposal for this directive has been severely criticized from the perspective of personal data protection,[42] the debate about data (in)alienability is still underdeveloped.[43] Below, we advance this debate.

I. Are Personal Data Inalienable?

The Digital Content and Digital Services Directive goes as far as to assert that "the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity".[44] Although this may indicate a clear political aspiration of EU leaders to exclude personal data from commerce, we think that black letter law is not as clear. Consider, for example,

[35]*E.g.*, Herbert Zech, *Data as a Tradeable Commodity—Implications for Contract Law*, in Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition (Josef Drexl ed., 2018); De Franceschi, *supra* note 1, at 5.

[36]Directive 2011/83/EU, of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, 2011 O.J. (L 304) 64.

[37]Regulation (EU) 2018/1807, of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, 2018 O.J. (L 303) 59.

[38]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 O.J. (L 136) 1.

[39]Regulation (EU) 2018/1807 at recital 7.

[40]Directive (EU) 2019/770 at Article 2(1).

[41]Directive (EU) 2019/770 at Article 3(1).

[42]*See, e.g.*, *Opinion of the European Data Protection Supervisor on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content* (Mar. 14, 2017), https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf; Romain Robert & Lara Smit, *The Proposal for a Directive on Digital Content: A Complex Relationship with Data Protection Law*, 19 ERA F. 159 (2018).

[43]*See also* Gianclaudio Malgieri & Bart Custers, *Pricing Privacy—the Right to Know the Value of Your Personal Data*, 34 Computer L. & Sec. Rev. 289 (2018); Gianclaudio Malgieri, *"User-Provided Personal Content" in the EU: Digital Currency between Data Protection and Intellectual Property*, 32 Int'l Rev. L., Computers & Tech. 118 (2018).

[44]Directive (EU) 2019/770 at recital 24.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

how the EU Charter of Fundamental Rights (the Charter) addresses personal integrity and personal data protection. While Article 3(2) affirms that body parts cannot be "a source of financial gain", and thus sends a clear message regarding trade in human organs, Article 8 merely declares that everyone has the right to the protection of personal data concerning her. It does not prohibit financial gain from one's own personal data, which suggests that the Charter does not take any position in relation to (in)alienability of personal data.

As regards personal data in general and their being in the nature of inalienable goods, we should take into account EU secondary law (in particular the GDPR) and national data protection legislation. We also need to acknowledge that among personal data, there are some special categories of personal data (hereinafter *sensitive data*, that is data revealing racial or ethnic origin, political, religious or philosophical beliefs, trade union membership, or genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, or data concerning sex life or sexual orientation of the data subject) whose processing is limited to even more restricted cases (Article 9 GDPR, see more below).

The GDPR does not explicitly address inalienability of personal data or their nature as *res extra commercium*. Nor does it use the terms "trade" or "sale" when referring to personal data. However, the centrality of the data subject as a holder of inalienable data protection rights—the right to access, the right to object to processing, the right to withdraw the consent, the right to erasure, the right to portability—seems to be the first relevant element to be considered. It is true that personal data can be processed on the basis, among others, of consent and contract and that these are two elements that could also justify tradability of personal data. Nevertheless, consent should be free and revocable (Article 7 GDPR).

Revocability of consent is thus an apparent index of the not-fully-tradable nature of personal data.[45] In addition, Article 7(4) states that, "[w]hen 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". In other words, when consent to data processing is given merely as a counter-performance in exchange for the provision of a service, one may doubt the freedom with which consent is given.

The wording of Article 7(4) GDPR has triggered a vivid debate about its proper interpretation. On the one hand, commentators largely recognize the nature of data as a *de facto* price, consideration, or counter-performance in the digital market.[46] On the other hand, Article 29 Data Protection Working Party (Art 29 WP)—which was an independent European working party that dealt with issues relating to the protection of privacy and personal data before the entry into application of the GDPR—has explicitly affirmed that personal data can never be "counter-performance", thus strengthening the argument that personal data should not always be considered alienable.[47] However, Art 29 WP seems to accept that personal data may be monetized if specific conditions are respected. In particular, data can be monetized if the controller offers to the data subject a *genuine choice*:

> between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand.[48]

[45] *See* GDPR at recital 42 ("Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.").

[46] *See, e.g.*, Malgieri & Custers, *supra* note 43, at 285, 292, 306, 307. *See also* Axel Metzger et al., *Data-Related Aspects of the Digital Content Directive*, 9 JIPITEC 90 (2019).

[47] *See Guidelines of the Article 29 Data Protection Working Party on Consent Under Regulation 2016/679*, at 8 (2018) ("[T]he GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."). *See generally* Robert & Smit, *supra* note 42; *Opinion*, 2017, *supra* note 42.

[48] *Guidelines*, 2018, *supra* note 47, at 9.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

Further, Art 29 WP remarks that "both services need to be genuinely equivalent".[49] One might wonder whether a premium service upon payment and a free service upon accepting additional purposes of data processing could ever be "genuinely equivalent" alternatives. Still, if there is—at least in principle—the possibility of accepting a service delivered by the controller without consenting to the additional data use in question, then the consent could be considered genuinely free.

These considerations seem to suggest that, in principle, the data subject should not be asked to disclose her personal data in exchange for money or as an alternative to money. But if her will is genuinely free, that is if the expressed consent is not conditional (Article 7(4) GDPR), it is possible that personal data are monetized. Of course, the consent can be always withdrawn (Article 7(3) GDPR).

Accordingly, we submit that the flow of personal data is based on a limited alienability rule: Personal data can be traded in exchange for a monetized service only if specific conditions are met.[50]

Interestingly, at least two European Member States' legislation implementing the GDPR—that of the UK and of Denmark—mention the wording "sale of personal data". The UK Data Protection Act 2018, similarly to the UK Data Protection Act 1998, prohibits the "sale of data" as part of the crime of "unlawful obtaining of personal data".[51] In particular, it is prohibited to sell data or offer to sell data that have been obtained without the consent of the data controller. However, these provisions criminalize only business-to-business—or more accurately, controller-to-controller—data trading. What is protected here is the consent of the data controller to commercialize personal data that were lawfully obtained and processed.

The UK Data Protection Act 2018 would seem to imply that any sale of personal data is permitted and lawful, provided that the first data controller consents. But that would be a misunderstanding of what the law demands. According to the GDPR, the exchange of personal data from one data controller to another data controller must respect the data protection principles. Namely, the transaction must have a legal basis according to Article 6 GDPR, such as the data subject's consent or necessity of processing, discussed further in Section C.II.2, and the data subject should be informed about any recipient of the personal data (Articles 13(1)(e) and 14(1)(e) GDPR). If and only if all the GDPR safeguards are respected, then the exchange of personal data between two data controllers is permitted, even if that exchange is monetized. In other words, we think we can already affirm at this point that personal data are based on a limited alienability rule.

The same argument must apply to other national legal systems in the EU, including Danish law. The Danish Data Protection Act states that:

> [D]ata controllers who *sell lists of groups of persons* for direct marketing purposes or who print addresses or distributes messages to such groups on behalf of a third party may only process: (1) [D]ata concerning name, address, position, occupation, e-mail address, telephone and fax number; (2) data contained in trade registers which according to law or provisions laid down by law are intended for public information; and (3) other data if the data subject has given explicit consent.[52]

This confirms the possibility of trading personal data, but, again, only where the data protection principles set out above are met.

In order to understand tradability of personal data, it is instructive to look outside the EU, for instance to California's Silicon Valley. Presumably, European businesses would want to trade data with innovative entities incorporated there. California law seems to recognize personal data as *res intra commercium*. In the California Consumer Privacy Act 2018 (CCPA), for instance, the

[49]*Guidelines*, 2018, *supra* note 47, at 9.

[50]*Cf* Ariel Porat & Stephen D. Sugarman, *Limited Inalienability Rules*, 107 GEO. L.J. 701 (2019).

[51]Data Protection Act 2018, c. 6, s. 170 (UK).

[52]Databeskyttelsesloven [Data Protection Act], part 3, § 13(5) (2018) (Den.), *translation at* https://perma.cc/7TBD-YW7W (emphasis added).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

concept of "sale of personal data" is largely accepted as the basic rule in the relationships between different data controllers.[53] In addition, such sale of data is recognized as the basic rule, while individuals have only the right to be notified that their data will be sold and the right to opt out from any sale of data relating to them.[54] The rights of notification and opt-out seem similar to the requirements of information disclosure and legal bases in the GDPR (Articles 14 and 6) as described above. Thus, alienability of personal data is arguably also limited in California.

Interestingly, the CCPA even seems to declare an absolute inalienability rule. Section 2 of the CCPA acknowledges that "the right to privacy is among the 'inalienable' rights of all people". The same section further clarifies the content of such inalienable right: "Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information". In other words, the inalienable right to privacy includes the right of individuals to limit the trade of data related to them. Overall, we thus submit that one can identify a limited alienability rule for personal data even in the US.[55]

A similar declaration of inalienability can be found in the Quebec Civil Code, in which Article 3 affirms that: "[E]very person is the holder of personality rights, such as the right to [. . .] privacy. These rights are *inalienable*".[56] Even in this case, inalienability does not refer to market inalienability of personal data as *res extra commercium*, but to the right to privacy as a right that cannot be removed from individuals.

In sum, the analysis of personal data as *res extra commercium* is complicated; their nature as an (in)alienable commodity might appear ambiguous in many legal frameworks. Regardless of definitions and pronouncements in legal documents, however, if we focus just on the possibility of processing personal data on a monetization basis—either the data controller asks the data subject for personal data in exchange for money or for a valuable service, or the data controller exchanges personal data with a third recipient, such as a business, in exchange for money—we conclude that there is a limited alienability rule. In the following sections we will summarize the limits for trading personal data under EU law.

II. Trading Personal Data under the GDPR: Conditions and Uncertainty

In order to understand the conditions under which the GDPR allows trade in personal data, we should first clarify what "trading data" means and then differentiate amongst relevant scenarios. We accept here that trading data means obtaining personal data in exchange for money or for other valuable assets such as digital services or valuable information. Two different scenarios should be addressed here: Primary data trade where the data controller obtains personal data from the data subject, and secondary data trade where the data controller exchanges personal data with a third recipient, such as a business that can thus become a second data controller.

In both primary and secondary data trade, the trader(s) need to consider two variables: (1) The nature of data—are they personal or non-personal data? If they are personal data, are they sensitive or non-sensitive data?; (2) The legal basis for trading data—what is the legal basis and when does it change? We will discuss these variables in the following two sections of this Article.

1. The First Variable for Limited Alienability of Data: The Dynamic and Uncertain Nature of Data

Regarding the nature of data, Article 4(1) GDPR clarifies that "personal data" means any information relating to an identified or identifiable natural person. Interestingly, recital 26 of the GDPR explains

[53]Section 1798.140t(1) clarifies the concept of "sale" in relation to trade in a consumer's personal information. Just as in the UK and Danish data protection laws, in Californian law the "sale" of personal data is mentioned only as a business-to-business practice.

[54]Consumer Protection Privacy Act, CAL. CIV. CODE § 1798.120 (2018) (USA).

[55]*See generally* Porat & Sugarman, *supra* note 50 (regarding the concept of limited inalienability and limited property rules).

[56]Civil Code of Québec, S.Q. 1991, c 64 (Can.) (emphasis added).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

that when determining whether a natural person is identifiable, "account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly". To ascertain whether some means are reasonably likely to be used to identify the natural person—the recital continues—"account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". If, considering reasonable efforts, it is not possible to link the information to a natural person, the information shall be considered anonymous.[57]

As discussed in Section B, it appears clear that the nature of data is relative. Several variables, such as reasonable costs, time, or available technology, significantly affect our realistic capacity to single out individuals.[58] The CJEU in *Breyer v. Germany* recently clarified that data are anonymous not just if it is technically unfeasible to identify the natural person to whom they are related, but also if it is legally unfeasible.[59] In particular, if there are no legal channels for obtaining the "identifiers" that would turn those "anonymous" data into "personal" data, personal data shall be considered anonymous.[60] Owing to a broad interpretation of the CJEU's statement, it is sometimes thought that pseudonymous data (personal data separated from identifiers)[61] could also be considered anonymous data for a third party that cannot technically or legally access the identifiers.[62]

It is noteworthy that the nature of data also varies across time. For example, advancements in technology could make it easier to reidentify some originally anonymous data, or a party processing anonymous data could *ex post* obtain the identifiers in a lawful way. Thus, it should be accepted as a given that the nature of data is not only uncertain for traders at the moment of the trade, for example when it is not clear whether some data are really anonymous or relatable to an identifiable person, but also dynamically uncertain in the future, as anonymous data might become personal data.

Once it has been verified that traded data are personal data under the GDPR, another test should be performed to find out whether those data are of a sensitive nature. This extra categorization is necessary in the context of trading data because Article 9(1) provides for stricter rules for processing sensitive data. Accordingly, sensitive data are based on a more limited alienability rule than personal data generally.

For the reasons given above, the border between sensitive and non-sensitive data is uncertain, relative, and dynamic.[63] In particular, it has been affirmed that in the age of Big Data, machine learning, and data mining, it becomes increasingly easier to infer sensitive information from

[57]Luca Bolognini & Camilla Bistolfi, *Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulation*, 33 COMPUTER L. & SEC. REV. 171 (2017).

[58]Frederik Z. Borgesius, *Singling Out People Without Knowing Their Names—Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation*, 32 COMPUTER L. & SEC. REV. 256, 260 (2016).

[59]ECJ, Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, Judgment of 19 Oct. 2016, paras. 46, 47.

[60]*Id.* at para. 47.

[61]*See* Article 4(5) GDPR ("'[P]seudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.").

[62]*See* Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice* 13 (2012); Miranda Mourby et al., *Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK*, 34 COMPUTER L. & SEC. REV 222, 225 (2018).

[63]*See, e.g.*, Dara Hallinan, Michael Friedewald, & Paul de Hert, *Genetic Data and the Data Protection Regulation: Anonymity, Multiple Subjects, Sensitivity and a Prohibitionary Logic Regarding Genetic Data?*, 29 COMPUTER L. & SEC. REV 317 (2013); Gianclaudio Malgieri & Giovanni Comandé, *Sensitive-by-Distance: Quasi-Health Data in the Algorithmic Era*, 26 INFO. & COMM. TECH. L. 229 (2017).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

apparently non-sensitive data.[64] All personal data have a certain degree of intrinsic sensitiveness and an inversely proportional computational distance from sensitive information.[65] How this distance can be covered depends on advancements in technology, but also on the collection of further data. For example, our health conditions can be statistically predicted even from our daily location data. Accordingly, data traders should not only consider the uncertain and dynamic nature of data, but also the uncertainty and dynamism of the subcategory of sensitive data, which have implications for the legal bases for trading data.

2. The Second Variable: Legal Bases for Primary Data Trade

Insofar as data qualify as personal data or even sensitive data, data traders need a legal basis for the commercial exchange of such data. Legal bases for processing personal data are listed in Article 6 GDPR. For sensitive data there is an additional and more demanding list of conditions in Article 9 GDPR.[66]

Let us consider personal data first. We will focus on consent, a contract, and a legitimate interest as the potential bases for trading data lawfully (Article 6(1)(a), (b), (f) GDPR).[67] As mentioned above, consent, can serve as a legal basis for collecting data for monetization purposes.[68] However, according to Article 7, this consent must be unambiguous, fully informed, including being informed of the commercial purpose of the data processing, and it must be revocable and free, meaning not conditional on the provision of services with no other genuinely equivalent alternatives. Accordingly, businesses who trade personal data must ascertain that consent has been provided unambiguously, that it was informed, free, and that it remains valid. The consent remains valid if it has not been withdrawn by the data subject.

Another legal basis for monetizing personal data could then theoretically be a contract, but commentators have dismissed this possibility.[69] Even Art 29 WP has clarified that the provision of Article 6(1)(b) GDPR, stating that processing is lawful if it is "necessary for the performance of a contract to which the data subject is party", "must be interpreted strictly and does not cover situations where the processing is not genuinely *necessary* for the performance of a contract, but rather unilaterally imposed on the data subject by the controller".[70] Art 29 WP thus effectively excluded the use of contract as a legal basis for processing data for monetization purposes, including marketing purposes.[71] We agree with Art 29 WP's view.

[64]Giovanni Comandé & Giulia Schneider, *Regulatory Challenges of Data Mining Practices: The Case of the Never-Ending Lifecycles of "Health Data,"* 25 EUR. J. HEALTH L. 284 (2018). *See also* Effy Vayena & Urs Gasser, *Strictly Biomedical? Sketching the Ethics of the Big Data Ecosystem in Biomedicine*, *in* THE ETHICS OF BIOMEDICAL BIG DATA 20–24 (Brent Mittelstadt & Luciano Floridi eds., 2016).

[65]Malgieri & Comandé, *supra* note 63, at 230, 240. *See also Annex to the Letter from the Article 29 Data Protection Working Party to the European Commission* (Feb. 5, 2015), at 5.

[66]*See also* Elena Gil González & Paul de Hert, *Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data—An Analysis of GDPR Provisions and Principles*, 20 ERA F. 1.

[67]We do not discuss the possibility to "monetize" data on the basis of a legal obligation to which the controller is subject (Article 6(1)(c) GDPR), vital interests of the data subject (Article 6(1)(d) GDPR), or a performance of a task carried out in the public interest (Article 6(1)(e) GDPR), because these bases do not fit the private commercial nature of data trade which we want to address.

[68]*See Opinion of the Article 29 Data Protection Working Party on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, 2014 W.P. 217 (2014). *See also* Frederik Borgesius, *Personal Data Processing for Behavioural Targeting: Which Legal Basis?*, 5 INT'L DATA PRIVACY L. 163, 176 (2015).

[69]CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 234–35 (2d ed. 2007); Borgesius, *supra* note 68, at 170.

[70]*Opinion*, 2014, *supra* note 68, at 16 (emphasis in original).

[71]*Opinion*, 2014, *supra* note 68, at 17:

> [Contract] is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

The last variant is a legitimate interest as a basis for lawful processing of personal data. Pursuant to Article 6(1)(f) GDPR, this could be where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject". This legal basis thus requires us to take account of several tests, including the necessity test; the legitimacy test; and the balancing test, considering the counter-interests of the data subject.[72]

The use of "legitimate interest" as a legal basis for monetization purposes is problematic,[73] especially with regard to the necessity test. Art 29 WP has indeed clarified that data controllers should "consider whether there are other less invasive means to reach the identified purpose of the processing and serve the legitimate interest of the data controller".[74] In data trade, the identified purpose might be an economic profit from personal data, but such a purpose would probably be considered insufficiently specific to meet the necessity test.[75] In addition, one could always argue that the desired economic profit could be achieved through less invasive means, such as when the content providers would provide some premium services upon a payment.

The legitimacy test allows for more freedom and can be interpreted expansively.[76] Still, the interest must always be lawful, sufficiently clear, and represent a real and present interest.[77] Finally, the balancing test[78] should take into account the controller's legitimate interest, impact on the data subjects such as intrusiveness of profiling, provisional balance, and additional safeguards applied by the controller to prevent any undue impact on the data subjects—transparency, ease of exercising the right to object, et cetera.[79]

All these considerations make it extremely difficult to use the category of legitimate interest as a legal basis for trading personal data. It will be necessary to evaluate on a case-by-case basis whether a specific data transaction involves intrusive profiling, unclear information about purposes or commercial implications, alongside other legal requirements. And even though "[t]he processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest", as is confirmed in recital 47 of the GDPR, the data subject has the right to object at any time to such processing (Articles 21(2) and 21(3) GDPR). Accordingly, the legal basis for data transactions could be invalidated *ex post*, which seems to be very similar to the right to withdraw consent in case of processing based on consent.

In addition, if the traded data are not only personal, but also sensitive (Article 9(1) GDPR), they can never be processed merely for legitimate interest purposes, because under Article 9 GDPR there is no reference to legitimate interest as a legal basis for processing. In that case, just two legal bases might in principle be adequate for the processing of sensitive data for monetization purposes: (1) When the data subject has given "explicit consent for one or more specified purposes" (Article 9(2)(a) GDPR), given that the consent is free, informed and revocable (Article 7 GDPR); or (2) when processing relates to "[sensitive] data which are manifestly made public by the data subject" (Article 9(2)(e) GDPR). In this second case, however, we observe that if personal

[72]*E.g.*, Gabriela Zanfir-Fortuna, Deciphering 'Legitimate Interests': Report Based on More than 40 Cases from Practice 5–7 (2018).

[73]Borgesius, *supra* note 68, at 170.

[74]*Opinion*, 2014, *supra* note 68, at 55.

[75]*See Opinion 3/2013 of the Article 29 Data Privacy Working Party on Purpose Limitation*, 2013 W.P. 203, at 16 (2013) ("For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience,' 'marketing purposes,' 'IT-security purposes,' or 'future research' will—without more detail—usually not meet the criteria of being 'specific.'").

[76]*See Opinion*, 2014, *supra* note 68, at 24.

[77]*Opinion*, 2014, *supra* note 68, at 25.

[78]*See* Irene Kamara & Paul de Hert, *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, in Cambridge Handbook of Consumer Privacy (Evan Selinger, Jules Polonetsky, & Omer Tene eds., 2018).

[79]*Opinion*, 2014, *supra* note 68, at 33.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

data are already made public, this might lower their commercial value for data traders because they would not need to buy these data, they just would need a technology to collect them. Still, even in this second case, it is worth remembering that for processing sensitive data, controllers need a legal basis under both Articles 9 and 6 GDPR, because sensitive data also count for personal data.[80] Therefore, in the case of processing sensitive data which were manifestly made public by the subject, the data controller should either seek the consent of the subject under Article 6(1)(a) or prove that there is necessity for a legitimate interest under Article 6(1)(f). The route of a legitimate interest then poses multiple hurdles, namely the legitimacy test, the necessity test, and especially the balancing test when trading sensitive data for merely commercial reasons.[81]

Overall, we submit that this second variable is also uncertain and dynamic. In cases of consent, even when the data traders pass the freedom of consent test, consent could be withdrawn in the future.[82] In cases of legitimate interests, even when the data controllers pass the necessity, legitimacy and balancing tests, the data subject could easily object to data processing and thereby delegitimize it. With regard to the secondary data trade, that is a commercial exchange of data between two data controllers such as a service provider and an advertising company, the same conditions apply. In addition, it might be necessary to obtain a separate consent for exchanging data with a third party: Art 29 WP clarified that in order to respect the principle of "granularity", the data controller that processes data for her own purposes must ask for a separate consent to communicate the data to a third party.[83]

3. Dynamically Limited Alienability Rule for Personal Data under the GDPR

Given the evidence in the legal sources and literature set out above, we conclude that personal data are not based on an inalienability rule and are, therefore, not *res extra commercium*. Nonetheless, we also conclude that strict conditions apply to the commercial flow of personal data, and so we can talk about a *dynamically limited alienability rule* in relation to personal data.

Figure 1. (see below) visualizes how this complex rule might look. Accordingly, the GDPR arguably forbids trade in data when:

1. Data are personal data from the outset or become personal data subsequently AND there is:
   a. No free consent of the data subject under Articles 6(1)(a) and 7 GDPR; or
   b. No necessity for a legitimate interest under the conditions of Article 6(1)(f) GDPR for processing those data;

   OR

[80] *Opinion*, 2014, *supra* note 68, at 15 n.31 ("Publicly available data are still personal data subject to data protection requirements, including compliance with Article 7 [of the Data Protection Directive, now Article 6 GDPR], irrespective whether or not they are sensitive data.").

[81] *See Opinion*, 2014, *supra* note 68, at 35 (affirming that when processing data for purely consumer profiling reasons, "the inference of sensitive data (health data) [. . .] contributes to tipping the balance in favor of the data subject's interests and rights"). *See also Opinion*, 2014, *supra* note 68, at 59 (discussing an example of an on-line pharmacy performing extensive profiling). *See generally*, *Opinion*, 2014, *supra* note 68, at 38–39 (arguing that processing sensitive data—or even data that could reveal sensitive data—contributes to set the balance test in favor of the data subject because "the more sensitive the information involved, the more consequences there may be for the data subject").

[82] In this case, the processing of data before withdrawal is not unlawful (Article 7(3) GDPR), but no new processing of such data is allowed. At the same time, if there are no more legal bases, such data should be erased. *See Opinion 3/2019 of the European Data Protection Board Concerning the Questions and Answers on the Interplay Between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (Art. 70.1.b)*, at 7 (Jan. 23, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

[83] *Guidelines*, 2018, *supra* note 47, at 10.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

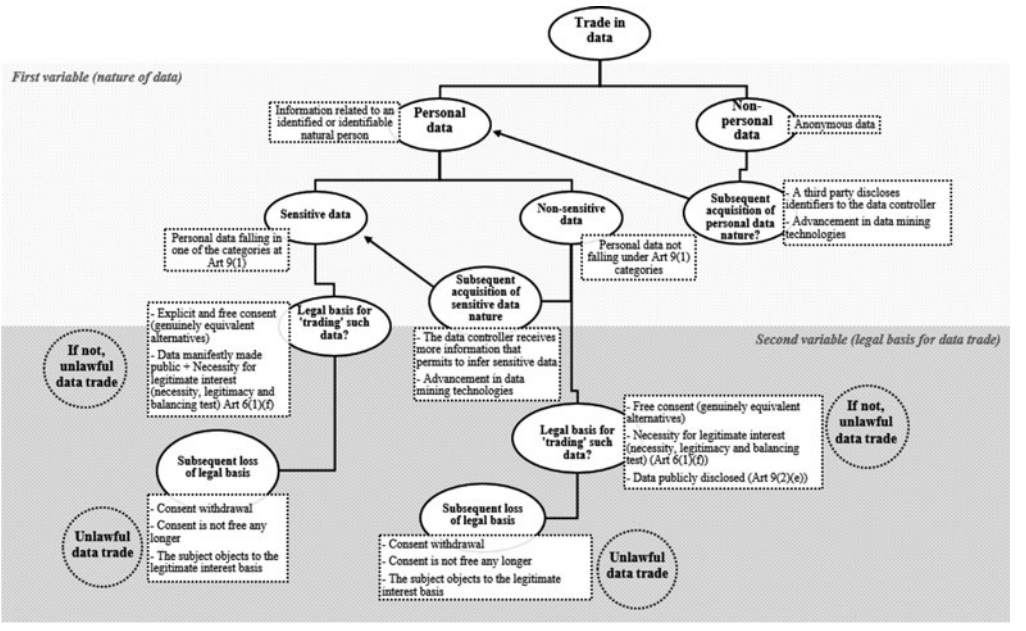

Figure 1. Dynamically Limited Alienability Rule derived from the GDPR and explaining conditions under which personal data can be traded.

2. Personal data are also sensitive data according to Article 9(1) GDPR from the outset or become sensitive data subsequently, AND:
   a. There is no free consent of the data subject under Article 9(2)(a) and Article 7 GDPR; or
   b. Those data are not manifestly made public by the data subject or, even if made public, there is no necessity for a "legitimate interest" under the conditions of Article 6(1)(f) GDPR for processing those data;

   OR

3. The legal basis is subsequently lost, for example:
   a. Consent is withdrawn or loses its required qualities (Article 7 GDPR); or
   b. In case of legitimate interest basis, the data subject objects to the processing of personal data (Article 21 GDPR).

D. The Two-Stage *Data Extra Commercium* Test

While Roman law provided a clear and principled test that helped indicate when contracting parties should be held responsible for illicit transactions in *res extra commercium*, and consequently when the parties' commercial interests are to be protected by legal remedies,[84] current law does not feature any similar test in relation to data. The Digital Content and Digital Services Directive provides consumers with some contractual remedies and deals with some aspects of onward data transfers to third parties,[85] but it is does not address these issues in a complex and principled way

[84]*See* J. INST. 3.23.5. *See also infra* Section B of this Article.
[85]*See* Directive (EU) 2019/770 at recitals 24, 67, and Article. 16.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

that would be useful also for business-to-business contracts. This section fills this gap and proposes a test that is specifically designed for transactions in *data extra commercium*. We suggest that this test be thought of as a reasonable proxy on the basis of which national contract laws can be interpreted in accord with EU law limits on trade in personal data.

We already know that the Roman law *res extra commercium* test struggles to identify data that cannot be traded. To this extent, we suggest replacing the test with the *dynamically limited alienability rule*. As far as the legal implications of there being *data extra commercium*, however, the Roman law doctrine can play an important role. We can make a connection between the doctrine of *res extra commercium* and *data extra commercium* by focusing on the principles that underpin the Roman law test for inalienability of things. It is safe to assume that the test was underpinned by the following set of abstract principles that are based on the authority of reason: (1) If a contracting party—for instance an innocent buyer—is not responsible for the forbidden trade, it would not be unjust to provide that party with a remedy for the spoiled commercial transaction; (2) if the other party—for instance a fraudulent seller—is responsible for the mischief, the law could grant the innocent party a remedy against the defaulter; (3) otherwise, the contract is void and the law protects only the noncorrelative interests vested in the object of trade. The parties are responsible for the void transaction if they knew, or should have known, that the object was *extra commercium*. Let us translate these principles into the context of data.

The dynamic nature of data implies that all contracting parties can, in full awareness of the factual circumstances of their transaction, foresee that the relevant data may eventually be excluded from commerce on the basis of the reasons outlined in Section B and as demonstrated for trade in personal data in Section C. It could thus be argued that all parties should have known this potential status of the data and, accordingly, would all be responsible for the void or ineffective contract and its consequences. This line of thought would result in legal protection of *data extra commercium* only. No party would be entitled to a remedy.

The difficulty is that such a strategy does not take into account the legitimate interests and reasonable expectations of the parties. For example, it seems unreasonable to expect that a data subject will be able successfully to claim her interests and withdraw her consent in relation to fully anonymized data or to personal data that are collected and processed in the public interest.[86] Similarly, it would be unreasonable to assume that data regarding levels of humidity around the globe would be eventually analyzed as personal data. In theory, it is possible, but seems as unlikely as the authors of this Article being tenured next year. You would hopefully struggle to say we are responsible for not being tenured next year. By the same token, it is unreasonable to assume that parties can have limitless responsibility for *data extra commercium*. Given the dynamic nature of data, it is also unreasonable to assume that the parties' limited responsibility is fixed at the time of the conclusion of a contract or another key event in the digital trade. According to this line of thought, the parties' limited responsibility should be dynamic, too.

In response to these issues, we propose to translate the corrective element of reasonableness[87] into the following two-stage test. Stage 1: A party is responsible for trade in *data extra commercium* if and when, given the current state of knowledge and technology that is normally available to a person in a similar position, it is reasonably likely that the relevant data could reveal personal or other restricted information. Stage 2: If those conditions are met, the party cannot successfully escape responsibility for infringing on the values and interests in which trade is, or should be, legally prohibited. The party will be responsible for the mischief, unless that party demonstrates a special justifying reason, such as the data subject's free consent with

[86]*See* GDPR at Article 6(1) (giving a list of various acceptable grounds for lawful processing of personal data).

[87]Note that we do not regard reasonableness as a distinctly legal standard. *See, e.g.*, John Gardner, *The Many Faces of the Reasonable Person*, 131 L. Q. REV. 563.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

processing of personal data or a compelling legitimate interest of the controller, that serves as a defense to that party's liability for consequences caused by transactions concerning *data extra commercium*.

Stage 1 of the test protects reasonable expectations and legitimate interests in that the basic rule is that data are in commerce and the validity and enforceability of the contract should remain untouched, provided that there is no reasonably likely interpretation which would reveal that the relevant data embody values and interests that would be compromised by sale (as explained in Section B of this Article). Of course, the parties cannot prove negative facts, which is why the Stage 1 test must take a positive form as set out in the preceding paragraph. This positive test helps indicate whether the parties knew, or should have known, that any data in question are excluded from commerce. The "current state of knowledge" requirement allows us to consider the so far speedy developments in the field of data science. The requirement of "technology that is normally available to a person in a similar position" is designed to objectively indicate whether and when the relevant party could have discovered that the data qualify as *extra commercium*, and therefore whether and when that party has responsibility for trade in that data. This requirement is also justified by recital 26 of the GDPR.[88]

Stage 2 further limits the parties' responsibility in that it provides the parties with relevant excuses from responsibility and, consequently, defenses to liability. A party that becomes responsible at Stage 1 should prove that they have a relevant excuse that allows them to trade data that would otherwise be *extra commercium*. This could be freely given consent by the data subject or a compelling legitimate interest of the data controller winning the three tests—the legitimacy, necessity, and balancing tests—under Article 6(1)(f) GDPR. In the case of sensitive data, this could additionally be either explicit consent or demonstration that data were made public by the subject, or any other exemption provided by the law at the time when the party faces Stage 2. In this sense, Stage 2 reasonably limits responsibility for *data extra commercium* but does not deny it.[89]

If we now reconnect the two-stage test with its Roman law roots, we can see why the reasonable basic position of the law should be to protect only *data extra commercium* and the valuable information they embody. We can also see why it would often be the case that those who are in control of powerful analytic algorithms would be more likely to be responsible for *data extra commercium* than those to whom such tools are not available, typically consumers and data subjects. The question of specific legal sanctions and remedies is an important matter which we do not have space to open here. The key point is that the test could potentially be deployed in any type of data transaction and could be seen as a test that enforces requirements that are reasonable, principled, and in this sense non-arbitrary.

E. The Unique Benefits of the *Data Extra Commercium* Test

The two-stage test helps attribute responsibility for trade in *data extra commercium*, and thus also for the consequences of purporting such trade, in relation to both problematic scenarios set out in the introduction and Section B, that is in relation to *ex post* analytic exclusion of data from commerce and *ex post* withdrawal of consent. The same applies to the specific conditions of trade in personal data as discussed in Section C. These are undoubtedly unique and significant benefits that already justify why we should adopt the two-stage test in our thinking about data transactions in European contract law.

Here we want to highlight two practical benefits of the two-stage test. The first benefit relates to enforcement of the limited alienability rule in technologically advanced data trading and data

[88]*See supra* Section C.II.1.

[89]A detailed analysis of defenses and denials in relation to civil liability can be found in James Goudkamp, Tort Law Defences (2013) and Defences in Contract (Andrew Dyson, James Goudkamp, & Frederick Wilmot-Smith eds., 2017).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

processing systems where human end users are virtually out of the loop. Think, for instance, of "smart" environments and the Internet of Things. In order to deliver their functions, smart devices and their data processing algorithms often automatedly, and sometimes even autonomously, connect to other devices in order to transfer or process data. This can happen without the end user having any knowledge about such activity or the character of the data traded. Still, legal obligations can arise even in such autonomous environments and, likewise, the reasons for excluding some data from commerce apply there too.[90]

How then, if the human end users—who are traditionally considered the relevant contracting agents—are out of the loop, can we enforce the limited alienability rule? Consider, for instance, how difficult it would be to apply principles relating to defects of consent—mistake, fraud, threat, or undue influence—and misrepresentation in scenarios where the human user is out of the loop. Similarly, consider how difficult it would be to establish that the dynamic change of the nature of data amounts to an unforeseeable change of circumstances.[91] These issues demonstrate the obstacles relating to enforcement of the limited alienability rule when it comes to automated trading of data between autonomous agents. The existing European contract law tools are simply not designed for the infosphere where our traditional notions of time, space, and identity of objects start breaking down in relation to data and their informational properties.

This is where the two-stage test is likely to help. The law is well positioned to provide a legal, that is not technological tool to open black-boxed algorithmic trading systems, and thereby to protect the values and interests that certain types of data embody. The two-stage test could steer these challenges at the technological level by incentivizing development and implementation of suitable algorithms that would be designed to protect *data extra commercium*. Such protection by design could result in various auditing algorithmic protocols which would enforce the compliance with the law by computer code[92] that would flag up potential issues in the black box. Stage 1 of the test explains why it would be reasonable for stakeholders to use such auditing technologies and responsibly to develop the necessary technical standards.[93]

The second benefit relates to Stage 2 in that it demands development of adequate legal and technical standards for *ex post* authorization of processing of autonomously derived or inferred data. From a traditional European contract law perspective, trade in these derived or inferred data would be permitted if they were derived or inferred from *data in commercio*. The traditional contract law approach—we may call it a pre-Big Data or pre-infosphere paradigm—looks at data as a

[90]Notice the lack of literature addressing this fundamental shift and the inadequacy of existing contract law to address some of the implications of the "out of the loop" phenomenon. Rare exceptions are Marco Loos, *Machine-to-Machine Contracting in the Age of the Internet of Things*, *in* CONTRACTS FOR THE SUPPLY OF DIGITAL CONTENT: REGULATORY CHALLENGES AND GAPS 74–79 (Reiner Schulze, Dirk Staudenmayer, & Sebastian Lohsse eds., 2017) and Giovanni Sartor, *Contracts in the Infosphere*, *in* EUROPEAN CONTRACT LAW IN THE DIGITAL AGE 263–64, 271, 276 (Stefan Grundmann ed., 2018). *See also* Josef Drexl, *On the Future EU Legal Framework for the Digital Economy: A Competition-Based Response to the "Ownership and Access" Debate*, *in* TRADING DATA IN THE DIGITAL ECONOMY: LEGAL CONCEPTS AND TOOLS 232–34 (Sebastian Lohsse, Reiner Schulze, & Dirk Staudenmayer eds., 2017); Ruth Janal, *Fishing for an Agreement: Data Access and the Notion of Contract*, *in* TRADING DATA IN THE DIGITAL ECONOMY: LEGAL CONCEPTS AND TOOLS 271–72 (Sebastian Lohsse, Reiner Schulze, & Dirk Staudenmayer eds., 2017) (addressing the fact that a buyer of a smart device is out of the loop in relation to data transactions).

[91]*See* GARETH SPARK, VITIATION OF CONTRACTS: INTERNATIONAL CONTRACTUAL PRINCIPLES AND ENGLISH LAW (2013); JAN M. SMITS, CONTRACT LAW: A COMPARATIVE INTRODUCTION ch. 9 (2014); COMMENTARIES ON EUROPEAN CONTRACT LAW chs. 4, 6, 15 (Nils Jansen & Reinhard Zimmermann eds., 2018).

[92]*See* LAWRENCE LESSIG, CODE VERSION 2.0 83–153 (2006); Mireille Hildebrandt, *Law as Information in the Era of Data-Driven Agency*, 79 MICH. L. REV. 1 (2016); Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code of Law and Code* as *Law*, 82 MICH. L. REV. 207 (2019).

[93]*See* GDPR at Article 25; JEAN-PIERRE QUEMARD ET AL., GUIDANCE AND GAPS ANALYSIS FOR EUROPEAN STANDARDISATION (2018).

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

merely accidental form of goods, rather than as primary objects of transactions.[94] If the primary good is excluded from commerce, data are too; if not, data are *in commercio*. We already know, however, that the relationship between data and the information they embody is not this straightforward and that, once the human user is out of the loop, we could lose sight of trading data that should be excluded from commerce. In other words, even derived and inferred data might eventually infringe upon non-tradable values and interests as set out in Section B.

Again, this is where the two-stage test might help. The current European law addresses issues of *ex post* withdrawal of consent and, relatedly, the legal implications of this *ex post* exclusion of data from the relevant transactions, including some implications for onward transfers of such *data extra commercium* to third parties. By contrast, the two-stage test incentivizes development of reasonable legal and technical standards that would allow not only for exclusion of data from commerce but also for *ex post* authorization of such data and, accordingly, *ex post* inclusion of derived or inferred data in commerce. This second benefit is, again, characteristically significant for enforcement of the limited alienability rule in the era of Big Data and the infosphere and demands us to adopt some new contract law rules for attributing responsibility for *data extra commercium*. What shape these rules will take in national legal systems, or whether there will be pan-European standard terms or implied terms for business-to-business and business-to-consumer contracts, are questions ripe for further consideration that exceeds this Article.[95] Overall, the two-stage test could incentivize more efficient legal and technical standards for detecting and protecting *data extra commercium* even in fully automated and autonomous trading systems.

F. Conclusion

No matter how tempting the intellectual parallel may be, data are not *res extra commercium* and we should seek to avoid thinking about them in these terms. This does not mean, however, that data are *res in commercio*; that too would be a misunderstanding. The nature of data is more complicated than that and we cannot simply apply traditional concepts and contract law doctrines to them.

In this Article, we argued that transactions in data can be limited and that data are subject to what we call a *dynamically limited alienability rule*. In Section B we argued that the dynamically limited alienability rule can be explained on a principled basis and, therefore, applied more generally to trade in any data. In Section C, we demonstrated how this rule would apply in the context of the current laws regarding trade in personal data. We also visualized the rule in Figure 1, so that our readers might easily refer to it in their own work or legal practice. Further, Section D proposed and defended a general two-stage test that could help legal practitioners, judges, and lawmakers to determine when trade in data is illicit and who, if anyone, shall be held responsible for this mischief. Finally, we showed not only how the two-stage test and the limited alienability rule may help to link EU data protection laws with contract law rules and principles, but also how the test might help to enforce legal principles of *data extra commercium* in fully automated and autonomous data trading systems.

We thus proposed that *data extra commercium* be thought of as a dynamic concept for future European contract law or national laws implementing the Digital Content and Digital Services

[94]Even the paradigm adopted in Directive (EU) 2019/770 sees data as a mere carrier of some content which we want to trade. The traditional view can also be found in ECJ, Case C-128/11, UsedSoft v. Oracle, ECLI:EU:C:2012:407, Judgment of 3 July 2012, paras. 41, 61.

[95]For instance, von Westphalen talks about "default rules" for B2B contract regarding Big Data but in essence is talking about supply of digital content only. Friedrich Graf von Westphalen, *Contracts with Big Data: The End of the Traditional Contract Concept?*, *in* Trading Data in the Digital Economy: Legal Concepts and Tools 245, 259 (Sebastian Lohsse, Reiner Schulze, & Dirk Staudenmayer eds., 2017). For a similar position, *see also* Drexl, *supra* note 90, at 233.

https://doi.org/10.1017/glj.2020.47 Published online by Cambridge University Press

Directive. After all, in a world of speedy technological advancements and changes in business practices and models, it seems a more efficient and sustainable regulatory strategy to link contractual sanctions and remedies with the object that is traded—that is data—rather than with the specific types of contractual transaction. Besides, a standard requirement of commercial law is that the object of a transaction is lawful, and it would be difficult to conceive of the law permitting otherwise. For this reason, we coined the term *data extra commercium* and the two-stage test to help enforce the limited alienability rule pertaining to all data transactions. As such, *data extra commercium* may even serve as an elementary tool of data protection.[96]

[96]*See* Mireille Hildebrandt, *Primitives of Legal Protection in the Era of Data-Driven Platforms*, 2 GEO. L. TECH. REV. 252, 267 (2018).

Cite this article: Janeček V, Malgieri G (2020). Commerce in Data and the Dynamically Limited Alienability Rule. *German Law Journal* **21**, 924–943. https://doi.org/10.1017/glj.2020.47