# eLaw
# Working Paper Series

No 2019/003 - ELAW– 24 April 2019

## Big data analytics contracts
*A nexus between digital platforms' regulation & private law?*

Serge J.H. Gijrath

Universiteit Leiden
eLaw

# Big data analytics contracts: A nexus between digital platforms' regulation & private law?

Prof. dr. Serge J.H. Gijrath, eLaw@Leiden University[1]

## Abstract

The starting point for this Paper is the take-off of big data analytics in light of the EU Commission's desire to safeguard a fair, innovation-friendly business environment for and effective competition on digital platforms.[2] Following an introduction of big data and AI notions, the Paper considers whether the use of online tracking methods may lead to dichotomy in the data economy. To what extent does digital platforms competition impact the control over personal and non-personal data protection regulation? These questions cumulate into a discussion on the need for stakeholders to exercise control over data transfers and data transfer agreements (DTAs). At the core of this paper lies the question, whether it is time to empower private users to govern data processing through consumer law, rather than just through data protection law. In terms of big data contracts, the discussion whether (big) data qualify as property and who owns that property is rekindled. A supplementary question is whether consumer law may function as a powerful tool for data subjects against third parties who transfer, sell or process their data. Consideration is given to big data analytics (transfer or sharing) agreements. The final remarks aim at reconciling the different policy & legal goals.

***Key Words:*** Big Data Analytics Contracts; Consumer Protection; Data Ownership, Data Protection; Data Subjects; Digital Platforms Regulation, GDPR, Legal Qualification of Big Data; Private Law.

---

[1] Endowed professor of telecommunications and ICT law, elaw@Leiden, and attorney-at-law/partner, C-Legal, Amsterdam, the Netherlands. The author advises clients in the IT, media and electronic communications sector. He has no direct or indirect links to either the European Commission, Facebook or Cambridge Analytica. This article is based on independent research and reflects the objective findings and personal opinions of the author.

[2] Paper closed 10 April 2019. The author wishes to thank is colleague Karolina La Fors, post-doc researcher at Leiden University, for her insightful comments. This Paper extends the presentation at Universitat de València, "Reconciling Big Data Analytics Contracts with Digital Platforms' Regulation" to include private law notions; keynote speech, *Competition Law, Digital Platforms and Big Data, Conference Paper*, June 2018.

# 1. Introduction: Big Data, you are beautiful…

## 1.1 Context, research questions & structure

> "*Big data is no fad. (…) [T]he application of big data analytics has spread throughout the public and private sectors. Almost every day I read news articles about its capabilities and the effects it is having, and will have, on our lives. My home appliances are starting to talk to me, artificially intelligent computers are beating professional board-game players and machine learning algorithms are diagnosing diseases*."[3]

The UK Information Commissioner expressed these thoughts in a report of her office that discusses big data in the context of artificial intelligence (AI), machine learning and data protection issues. The ICO's comments underline the importance of considering the scope and depth of big data analysis, because it will impact tremendously the daily lives of data subjects (we all are data subjects).

The first two parts of this Paper set the stage: the data economy, digital platforms' regulation and personal data protection are the main themes. In this Paper, the providers of digital platform access and services will be labeled broadly as 'platform providers', also when they fall under the definition of online intermediaries.[4] Since the scope is on big data analytics contracts, I may use the term data policy as an alternative to privacy policy. A brief discussion of the different approaches to the data economy is held in para. 1.2. However, this article is not focused primarily on analysing the various competition law administrative actions against parties like Facebook; it desires to explore the transparency general terms and conditions as effective possibilities for **redress** when these terms and conditions are not respected in big data analytics.[5] Before diving into the legal issues in parts 2-4, a quick glance will be had at the 2018 Facebook Privacy Basics and Data Policy. The short overview of Facebook's policies is meant to show what the platform provider expects to do with private user data gathered at the entrance gate and beyond. The actual passing-on of their data, in whatever form or guise, is much more difficult to establish. Once the data are in the hands of

[3] Information Commissioner's Office, UK, *Big data, artificial intelligence, machine learning and data protection,* Report, v. 2.2, 20170904, 2017 (ICO 2017). Some definitions (big data; AI) were found in the footnotes of this report; reference is made to the original source and this writer's access thereto.

[4] See Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, COM(2018) 238 final, Brussels 26 April, 2018 (the draft Online Intermediary Services Regulation). See also Council Position, Press Release, of 29 November 2018. At the time of closing this Paper (10 April 2019), the Regulation had not yet passed.

[5] Draft Online Intermediary Services Regulation, 4th para.

a third party, whose business is adding value with big data analytics, what happens to the data becomes even murkier. The Cambridge Analytica (CA) example raises questions about the impact and relevance of arrangements in terms of accountability and contestability in big data analytics contracts between service providers and data analytics providers. Para. 2 discusses whether online tracking methods contribute to a dichotomy between digital platforms, data economy policy objectives and data protection regulation. This will end with a short reflection on whether there is a regulatory gap; and to what extent there is room for freedom of contract to reconcile regulatory concerns and practical considerations can be addressed in contracts.

The second part of this Paper discusses the autopoiesis between private and privacy law. Para. 3 reflects high-level on legal qualifications of data (including personal information) given by legal scholars. The common thread in this paper is private user/consumer/data subject empowerment against unwanted re-use, transmission and/or processing of their data. The Paper incorporates personal, pseudonymized or anonymized data and puts them against corporate (platform providers) claims on these data. Theories of property law, intellectual property law, freedom of information or currency notions are discussed. It will also be considered whether and how big data contracts fit into private law, in particular contract law.

More and more, data are digital. Returning to the concerns in the context of the CA case, para. 4 offers some thoughts on how the processing big data for analytics purposes could (and should) be regulated by applying private law notions. This Paper contends that, rather than private law supplementing data protection law, there should be a *nexus* between data protection law and private law to empower the private users to establish direct links with the parties who analyze their data, no matter the form of the data.[6]

## 1.2 Personal data and competition assessment

Free movement of data, as part of enhancing the internal market's data economy does not exclude a harmonized approach as to how private users can manage their data policies with

[6] This Paper thus also partly builds on legal research in that field; see, e.g., N. Helberger, F. Zuiderveen Borgesius and A. Reyna, "The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law", *Common Market Law Review* 54: 1427-1466, Kluwer Law International, 2017 (Helberger, Zuiderveen Borgesius, Reyna, 2017). The contribution predated the Cambridge Analytica incident and new draft regulation such as the draft Online Intermediary Services Regulation.

platform providers. As part of its Digital Single Market ("DSM") strategy, the Commission launched a competition sector inquiry into e-commerce in May 2015 to identify possible competition concerns arising from companies' online business practices.[7] Where data analytics companies utilise algorithms to process big data, this could result in restrictive agreements, decisions or concerted practices under article 101 TFEU. As can be inferred from the current EU investigations against digital platforms such as Google or Facebook, valuable big data that are not replicable may create anti-competitive market power for the party who controls the either the input data and/or the big data collection. The Commission also expresses concerns about access to these services and fears that innovation could be stifled.[8] It sees an imbalance in that the results of its E-commerce Sector Inquiry confirm the increased relevance of data. This also points to possible competition concerns relating to data-collection and usage. As an example, the Commission lists the exchange of competitively sensitive data, such as on prices and sold quantities, between marketplaces and third party sellers or manufacturers with own shops and retailers.[9] This could create competition concerns where the same players are in direct competition for the sale of certain products or services.[10] These seemingly conflicting concerns leads to a focus on regulation that promotes competition.

## 1.3 A little history of big data

The combination of big data, AI and machine learning is often called 'big data analytics'.[11] The proposal on the free flow of non-personal data applies a broad notion of data

[7] Commission, Final report on the E-commerce Sector Inquiry {SWD (2017) 154 final} COM(2017) 229 (Sector Inquiry 2017).

[8] Market Parties are asking for intervention. See, *i.e.*, G. Soros, "Only the EU can break Facebook and Google's dominance", *The Guardian*, 15 February 2018.

[9] Two examples: Commission Decision approval of the merger and subsequent fines in *Facebook/WhatsApp,* M.7217, 29.08.2014 and its decision in *Google Search Shopping,* Case AT.39740, 27.06.2017. The Commission imposed a hefty fine of € 2.42 billion to *Google* for abusing its market dominance as a search engine by giving an illegal advantage to another Google service, notably its comparison of shopping services.

[10] Sector Inquiry 2017, p. 14.

[11] Academics from different backgrounds use the term AI in one breath with 'machine learning'. In short, machine learning is a technical process that underpins and facilitates the use and output of AI. See also: "The Outlook for Big Data and Artificial Intelligence (AI)", *IDG Research*, 11 November 2016, https://idgresearch.com/the-outlook-for-big-data-and-artificial-intelligence-ai/ Accessed 21 March 2018.

processing. It includes data analytics services.[12] The ability to analyse data – for a given purpose, which can be anything – is considered as being valuable for society as a whole, because it could "*ultimately lead to better and more informed decisions.*"[13] Big data analytics can be used for businesses and governments purposes, *i.e.*, to monitor *human* behaviour, collectively and individually.[14] A definition is:

> "*[H]igh-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.*"[15]

Often, the characteristics of big data are determined by the possibilities that the mere volume thereof brings for analytical and statistical purposes. High-velocity is needed to process the gargantuan data volume and the variety of data to determine trends. Veracity of big data analytics is driven by the use of self-learning AI and machine learning.[16] AI is not intended for a linear analysis of data in the manner they have been processed or programmed. In general, AI consists of the analysis of data to model some behavioural aspects. Inferences from these models are used to predict and anticipate possible future events.[17] The added value of applying AI is that it is capable of learning from the data input. [18] Consequently, AI

---

[12] 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, OJ L 303/59, 28 November 2018, entry into force May 2019 (Free Flow of Non-Personal Data Regulation).

[13] European Data Protection Supervisor, "Meeting the challenges for big data, a call for transparency, user control, data protection by design and accountability", *Opinion 7/2015*, EDPS 19 November 2015 (EDSP 2015).

[14] "*Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms*"; Article 29 Working Party (WP29) *Opinion 3/2013* on purpose limitation.

[15] The latter part "decision making", currently is inciting most of the legal academic debate. See also: Gartner IT glossary Big data. http://www.gartner.com/it-glossary/big-data; accessed on 21 March 2018.

[16] J. Modrall, "Big Data and Algorithms, focusing the discussion", Oxford University, *Business Law Blog*, 15.1.2018 (Modrall 2018).

[17] UK Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making,* 9 November 2016 (ICO 2016).

[18] A recent OECD study qualified as a major risk of the use of algorithms that their application could assist the data analytics companies or their clients to sustain profits above the competitive level more easily without necessarily having to enter into an agreement; OECD, *Algorithms and Collusion – Background Note by the Secretariat*, DAF/COMP, (2017) 4 (OECD 2017), p. 24. At the same time, OECD signalled that it was difficult to draw conclusions on the technological question whether

may create intelligent responses to new data and adapt output accordingly. Let is first be established for the purpose of this article that, in many cases of big data analytics, personal data may not be involved. *Prima facie*, that could suggest that personal data protection issues are not a big concern. As will be seen below, that may be a false resolve. Input for big data analytics often is collected directly by the service provider from online customers or on the digital (social media) platforms they use. Batches of data are transmitted to third parties, where the delineation between personal and non-personal data blurs.[19] The analytics process enables the processor to mine data for new insights and to find correlations between apparently disparate datasets. However, big data analytics output is used also for purposes different from that for which it was collected. If the data analytics process is not managed well, then it can lead to disastrous consequences for private users. But, do the private users want to rely solely on privacy authorities' intervention?

## 1.4 When big data analytics go horribly wrong

In 2018, the perceived (ab-)use of data by big data analytics' companies proved to be a worrisome case of data being moved to third parties in contravention of personal data protection.[20] In 2019, the German Federal Cartel Office ('FCO', *Bundeskartellamt*) – following an investigation of Facebook into abuse of a dominant position – handed down a final ruling in first instance.[21] The FCO established that Facebook was limitlessly – and often without

algorithmic interaction can be considered as to be a "meeting of the minds" under the definition of agreement covered by competition rules, OECD 2017, p. 36-37 (OECD 2017).

[19] See also the data policy discussed in part 1 below. See on the policy: WP29 Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, 16 September 2014 (*WP 221*). Other relevant documents include: WP29 Opinion 03/2013 on Purpose limitation, WP 203; WP29 Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217; WP Opinion 05/2014 on Anonymisation Techniques, WP216. See also: Council of Europe. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 01/2017.

[20] By the end of 2018 the UK's ICO had imposed a fine of UKL 500.000 on Facebook.

[21] Bundeskartellamt, case B6-2216, 7 February 2019 (FCO 2019). See, *infra*, para. 1.4. At the time of closing this paper, the ruling was subject to appeal. It is very likely that the appeal will take place.

purpose – amassing every kind of data on its private users.[22] The FCO investigation relates to the way platforms with embedded Facebook APIs, as well as Facebook's subsidiaries, including WhatsApp and Instagram, shared the personal data of their private users. Besides being (1) data subjects within the meaning of the GDPR,[23] the subscribers to digital platforms and online intermediary services are: (2) the end-users of the content/services on such platforms, as well as (3) consumers (mostly).[24] Hence, they are referred to often in this Paper as 'private users.' The FCO's ruling provides an impressive legal novelty. More than before, the focus is on private users: the establishment of a dominant position combined with the absence of room to negotiate a privacy policy maybe somewhat of is a stretch. Teleologically, this assessment could prove to be very helpful for private users.

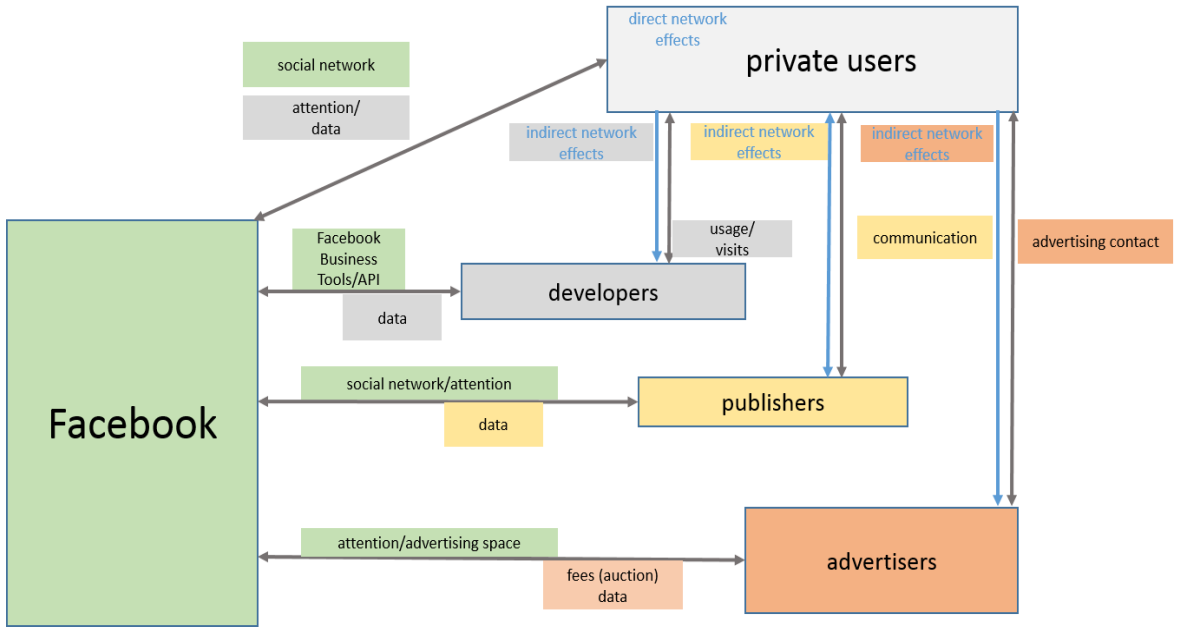
For the purposes of this Paper, Figure 1 (the table used by the German FCO in her anti-trust investigation of Facebook) is illustrative. It shows the nexus of contracts between Facebook, the private users (top right) and several third parties.

[22] "Private users" is the terminology used by the FCO. "Germany Restricts Facebook's Data Gathering", *NYT*, 7 February 2019. The commentator Labeled as a "novel anti-trust argument."

[23] See the General Data Protection Regulation, Council Regulation (EU) 2016/679 of 27 April 2016, *OJ L* 119/1, 4 May 2016 (GDPR).

[24] Clearly and arguably, there is interaction between (small) businesses on digital platforms as well; professional companies are less likely to benefit from a consumer law approach; but they do need to understand that they should contract for data use and sharing. See also: L. Determann, "No One Owns Data", *Hastings Law Journal*, vol. 70:1, 2019 (Determann 2019).

[**Figure 1**, © courtesy of the Bundeskartellamt, 7 February 2019]




The direct network effects are established on the basis of the relationship between Facebook and the private users. [25] Figure 1 reveals the data streams. It is clear that private users cannot be aware of the purpose and full scope of the data that is submitted to, or assembled and generated by, the platform provider. The only direct legal link for the private users is the arrow that goes to and from Facebook. In practice, there are at least three more links – but these are not subject to any transparent terms and conditions of data use. No matter the dark and sinister aims of CA, it was Facebook that transferred the data to CA – presumably under a data transfer agreement (DTA).[26] CA surfaced as the bad guy.[27] Ultimately, Facebook is

[25] The German FCO ruling is concise and very instructive. As regards CA: it was a US affiliate of a privately owned British company that specializes in the provision of data mining, data analysis and direct marketing services for application in the domain of public election processes. See, e.g., Linnet Taylor, "In the digital world we are all developing countries: what Cambridge Analytica can tell us about limited statehood in the West," in: *big data, justice*, internet article, 22 March 2018, https://linnettaylor.wordpress.com/category/big-data/. (Taylor, 2018) The company no longer exists. A criminal investigation was running against some the company's executives in 2019.

[26] For the sake of clarity, this paper uses the generic notion of data transfer, since that is what occurs in practice, and the agreement itself will contain scoping arrangements.

subject to legal scrutiny by several authorities. In terms of creating trust and control for big data analytics the question is: if Facebook shared personal information of hundreds of thousands private users, under what privacy policy or general terms and conditions did it inform them? What rights, if any, were granted to Facebook's private users whose data – whether or not with the use of pseudonymization or not were shared with third parties? Were these private users made aware sufficiently what these rights were and how to enforce them? What is the actual worth of personal data/privacy policies?

## 1.5 Just another boring set of personal data policies?

Private users are data subjects. Privacy policies are as boring as general terms and conditions. Most private users do not read them before purchasing services.[28] At the most, they browse through them. This may have to do with several circumstances: (1) data policies are boring. Many look the same, which makes the private users less vigilant; (2) data policies tend to be light on controller/processor obligations, and they are almost always non-negotiable; These high level statements also beg the question for the private users/data subjects: "Can I actually enforce my rights against the platform provider?" and (3) data policies tend to contain more disclaimers and controller rights than data subjects' rights. This could be hurdle to enforcement for the private user. Besides, the manner in which privacy policies are presented does not necessarily establish direct legal connections between the private user and the platform provider (Figure 1). Arguably, as fundamental rights, the data subject rights seem not that controllable.[29] The requirement of asking for (explicit) consent was never intended to bring long, impenetrable privacy policies. Nor was it designed to mean in practice that any data subject on social media would have the choice between 'consent' or not getting access to a service she desired. Before, consent implied a free and meaningful choice to say 'yes'. Consent implied that the data subject would be able to form a clear understanding of her rights. It should not entail that consent beforehand equals carte blanche for the platform provider.

---

[27] CA and Facebook were one focus of and enquiry by the ICO into data and politics, see also *The Guardian*, 17 March 2018. See also the investigation into politics, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

[28] See *Eurobarometer Special 447 on online platforms* (2016).

[29] H.U. Vrabec, Uncontrollable Data Subject Rights and the Data-driven Economy, dissertation, University Leiden, 2019 (Vrabec 2019).

In the data economy, consent may be overridden because of the platform provider's desire to collect big data for analytical or other commercial purposes. Many platform providers apply a whole series of principled "we make the world better" statements in their privacy policies.[30] But the private users lose track of the policies that apply to them and do not know with whom they are contracted. The publications on the CA backlash did not reveal immediately whether Facebook and CA had entered into an intricate data analytics, transfer, processing and/or other type of contract. The data subjects had not been informed properly of the purposes to aggregate personal data and match them with other personal data – often in the circle of trust of the first data subject. They could not ask CA or Facebook to cancel the process. Neither party offered transparency to any of Facebook's users on CA's processing and analytics methods and purposes. In the press there seems to be a consensus that, at some point, Facebook demanded that CA delete the personal data – we do not know how specific the demand was – of Facebook's private users. There also seems to be consensus that, not only did Facebook not follow-up on its demands against CA; it chose not to inform affected users proactively. According to its own policies, the only obligation Facebook had was to require strict confidentiality from CA. This assumes there was a form of DTA between them. Having gone over the applicable policies in February 2018, it seems that the legal basis for sharing data with third parties hinged on the following two provisions:

> "*Sharing With Third-Party Partners and Customers.*
> *We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.*"

And the following clause in its Data Policy (emphasis added):

> "*We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys."*

This provision was supplemented with a conveniently vague addition for Facebook:

[30] For this article, I looked at Facebook's Data Policy, https://www.facebook.com/about/privacy/. Accessed facebook.com on 23 March 2018.

> *"These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.*"

The wording is telling: The big data analytics company 'must' adhere to 'strict' confidentiality obligations. But did Facebook really agree this with CA? What agreements? Facebook may have idealized the "*big data: you are beautiful*" notion without having adequate regard to the private users justified expectations on data use; it did not establish any nexus between its general user terms and conditions and its privacy policies. More policies followed: considerations and a justification of Facebook submitting masked or aggregate personal data to third party companies. Facebook reassured that not the user's personal data, but "*non-personally identifiable information only*" would be shared with third parties;[31] these data would be shared "*for analytical purposes*". In hindsight, it can be established that CA generated quite different output from what was mentioned in the policies.

From a contractual perspective it begs the question whether Facebook can be held accountable directly by Facebook users for not enforcing the "strict confidentiality obligations" it mentioned in one of its policies. After the scandal broke, CA and Facebook were (and continue to be) subjected to various legal actions in a host of countries, mostly from semi-government agencies. The CA fallout could be overshadowed in the very near future by the more disruptions of data subjects rights that are unfolding in the data economy.[32] Applications such as Internet of Things (IoT),[33] Machine to Machine (M2M) communications and Blockchain and its Trust Protocol are just some examples of how data analysis is going to affect daily life. Big data analytics' possibilities really amount to the take-off and landing of everything and data mining is the tool.

# 2. a data economy & digital platforms

## 2.1 A big data economy while controlling digital platforms?

[31] The correct definition would be whether the data would or would not: "(…) *relate to 'an identified or identifiable natural person'*. Confer with the GDPR, recital (26).

[32] TNO, Ecorys, IVIR, *Digital Platforms: an analytical framework for identifying and evaluating policy options*, Report 2015 (TNO, Ecorys, IVIR, 2015); McKinsey Global Institute, *Disruptive technologies: Advances that will transform life, business and the global economy*, paper, May 2013. (McKinsey Global Institute 2013).

[33] WP29 Opinion 08/2014 on Recent Developments on the Internet of Things, WP223.

Data mining has become the new goldmining.[34] Several years ago, the Commission earmarked the data economy as a key objective in its Digital Single Market (DSM) strategy.[35] The Commission formulated concrete policy objectives that could be translated into regulation in order to achieve the internal market objective of a European data economy,[36] while creating a level playing field and a secure environment for big data analytics. The starting point was the stimulation of the potential of data for business, research and innovation purposes.[37] The Commission focused its policy on: (1) securing free flow of data within the Union;[38] (2) providing for data access and transfer;[39] (3) liability issues[40] and (4) data portability.[41] The regulatory focus on digital platforms is without prejudice to the rules related to the protection of personal data. But, the focus is devoid of any vision on empowering private users in enforcing their rights in civil courts, including by issuing liability claims – not the principles (art. 5) or provisions for consent (art. 7, but giving consent resembles offer/acceptance) but, rather, the data subjects' rights set forth in Chapter III GDPR, effectively and directly against the controller or various (sub-)processors. The

[34] Commission Communication "Building A European Data Economy" (Commission Communication 2017).

[35] https://ec.europa.eu/commission/priorities/digital-single-market_en; see also: Commission Communication "On the Mid-Term Review on the Implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All", {SWD(2017) 155 final}, COM (2017) 228 (Commission Communication DSM 2017).

[36] Commission Communication, "Building a European data economy", COM(2017) 9 final. Consultations ongoing. See also Commission Staff Working Document, accompanying the document Communication Building a European data economy {COM(2017) 9 final}, SWD (2017) 2.

[37] M. Granieri, A. Renda, *Innovation Law and Policy in the European Union, Towards Horizon 2020*, Springer, 2012 (M. Granieri, A. Renda, 2012).

[38] Free Flow of Non-Personal Data Regulation.

[39] Mostly the GDPR; although, arguably some of the digital platforms regulation contains comparable provisions, i.e., Regulation 2017/1128/EU of the European Parliament and of the Council of 14 June 2017 on Cross-border Portability of Online Content Services in the Internal Market, [2017] OJ L 168/1 including corrigendum to regulation 2017/1128; Regulation 2018/302/EU of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) no 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, [2018] OJ L 601/1; and fairly specific (and out of scope of this article), the languishing Directive 98/84/EC of the European Parliament and the Council of 20 November 1998 on legal protection of services based on, or consisting of, conditional access, [1998] OJ L 320/54.

[40] Under construction with different legal approaches competing, i.e., liability under the GDPR or contractual and extra-contractual liability; see below.

[41] This is part of the GDPR, see, e.g., articles 13 and 20.

problem present in parts of the GDPR is that not all controller/processor obligations are matched with data subjects' rights. Where they are – section 3, articles 16 (rectification) and 17 (erasure), article 18 (restriction on processing), article 20 (data portability) – the rights are often qualified and the burden of proof is not clear. This could make the private user's rights sometimes rather difficult to enforce in civil courts. Article 79 does open the door to various legal remedies, including administrative or non-judicial remedies, in the Member States.[42] Article 82 contains provisions on compensation and liability in case the personal data rights of the data subject have been breached. This could be the procedural law nexus with private law, but, to study the effectiveness requires more case law analysis. Some material provisions appear not easy to enforce: section 4, the right to object and automated individual decision-making (articles 21-22) contains fairly complex exclusions that are explained in detail in many of the extensive considerations.[43]

How does the GDPR connect with the Free Flow of Non-Personal Data Regulation? The latter is a high-level piece of regulation: it lays down rules relating to data localisation requirements, the availability of data to competent authorities and data porting for professional users. *Prima facie*, these are rather fragmented and specific objectives. Moreover, the definition of what are non-personal data leaves much to be desired. In fact, the Regulation contains no definition.[44] Rather than aiming at defining what non-personal data are, the Regulation provides some examples:

> *"Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines."* [45]

Article 6 draft Free Flow of Non-Personal Data Regulation – the provision on data porting – stipulates that the Commission must encourage service providers and professional users to

[42] See also Article 79 (2) on the competent court: "Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers."

[43] The GDPR contains only three considerations (20, 71 and 125) and they deal with varied issues.

[44] *Cf.* art. 3 of the Non-personal data Regulation: "'data' means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679;"

[45] Consideration (9) of the Free Flow of Non-Personal Data Regulation.

develop and implement codes of conduct detailing the information on data porting conditions (including technical and operational requirements) that providers should make available to their professional users in a sufficiently detailed, clear and transparent manner before a contract is concluded. The Commission will review the development and effective implementation of such codes within two years after the start of application of the Regulation on the free flow of non-personal data. The objectives of achieving a general right to data portability for non-personal data, a right to data access and liability for data (mis)use should be viewed in context. The Commission considers a data portability right first as a means to enhance competition, stimulate data sharing and avoid vendor lock-in. The underlying thought being that data access and liability will support data portability. Not that much has been written on the last two goals of promoting data portability and fostering liability. The Staff Working Document displayed the Commission's thought and concerns regarding liability, with mention of big data analytics.[46] Indeed, the Commission signals that the more complex use of data creates "highly complex" interdependencies, including with digital platforms. The considerations on possible liability for damages resulting from unlawful data analytics are still at a high level of abstraction. No thought is given on how damages claims would have to be enforced. If damages arise in the context of the use of new technologies, then this *should* at least lead to discussions on liability. These may range from legal issues regarding contractual, extra-contractual to risk liability. It is a welcome consideration to mention liability issues, but the liability concerns should be translated in clear, relatable and achievable policies and laws that offer some recourse to private users.

It will be challenging to align the different objectives and interests. There may be another dichotomy in the working here as may be inferred from the mid-term DSM strategy review.[47] The Commission wants to simulate data flows *and* it wants digital platform providers to inform their users more effectively what personal information and data is collected and how it is shared with and used by others.[48] Conversely, the analysis of the proposed instruments reveals a marked lack of a vision in terms of the economic value and model for big data analytics, their importance for the EU economy and the possible pitfalls of data analytics that are not supported by clear and enforceable data analytics agreements – including codes of

[46] Commission Staff Working Document 2017, p. 40*ff*.
[47] Commission Communication DSM 2017. On page 2, the Commission mentions a number of different activities ranging from: online advertising platforms, marketplaces, search engines, social media and creative content outlets, application distribution platforms, communications services, payment systems, and collaboration platforms.
[48] Currently Directives 95/46/EC and 2002/58/EC and once applicable, the GDPR.

conduct. Perhaps this is due to the circumstance that, with the exception of the Free Flow of Non-personal Data Regulation, the principal plans on stimulating the data economy are still under construction. It appears quite unlikely that data mobility and data portability regulation across the Union is going to improve; the draft Free Flow of Non-Personal Data Regulation does not provide clear and sustainable regulation that balances the different interests of the stakeholders, who can be (a group of) users/data subjects, professional data storage, digital platform or data analytics providers. The Commission mixes too many flavours and treats them equally.

## 2.2 Data mobility, control & trust

Articles 25 and 32 GDPR[49] and the consideration in the free flow of non-personal data regulation that personal data regulation (obviously) remains applicable is meant as a lever to safeguard that enhanced data for big data analytics purposes cannot be decompiled to reconstruct the personal data input.[50] Article 25 GDPR provides the regulatory requirement that must precede any form of big data analytics. The controller must take into account issues such as the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing. The general requirement that it must implement appropriate technical and organisational measures applies as well. Article 4 (5) GDPR emphasizes the definition of "pseudonymisation" to facilitate big data analytics by using data minimisation.[51] Hence, from the perspective of personal data regulation, there is a depository to build the big data economy on, and an added privacy check by prescribing data minimisation. The data must be surrounded by technical and organisational measures that prevent their deconstruction. More reliance on – and verification of – contractual arrangements between the digital platform service provider and the data analytics company may be necessary.

No matter that many big data processes do not always include personal data processing: big data analytics involve novel, complex and sometimes unexpected non-transparent uses

[49] See GDPR, recital (26).
[50] Article 40 GDPR prescribes a code of conduct.
[51] "'*pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject <u>without</u> 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.*"

of personal data.[52] it is necessary to have the parties involved make a privacy impact assessment ("PIA") beforehand in light of providing accountability to competition and data authorities. Elements of the PIA should include investigating whether the processing is fair and to what extent the processing could affect data subjects, and to determine measures to mitigate impact and strengthen control.

The tracking of online activity has become a revenue model for Internet service providers ("ISPs") and data analytics companies in the data economy. This development begs the question whether big data assembled from online tracking, should be considered personal even where anonymisation techniques have been applied. The reason is clear: it is likely that it is not that hard for the data analytics processing company to "*infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as on social media*".[53] In the Communication on Online Platforms and the DSM the Commission outlined the pros and cons of these platforms.[54] A concern is that the digital platform providers may have an inherent conflict of interest: while they play a key role in digital value creation, there is a blurring between service provision and the creation of significant value through data accumulation. Rather than considering what the implications may be for data analytics processes, the Commission refers to the GDPR only, and then considers the benefits of data analytics for its own goals of ensuring "*a data-driven public sector."*[55]

For the above reasons – lack of trust and no clear view yet on liability – the EU institutions are concerned about the loss or lack of control by the data subject. The Commission seems to think that detailed regulation could clash with the desire to stimulate the DSM. But trust is key. There are two levels of trust: (1) trust by users in the processing of their personal information by digital (or online) platforms, *and* (2) trust between a digital platform service provider, who enters into a form of contract with a third party service provider, who will perform big data analytics using data assembled by the digital platforms provider.

---

[52] *Cf*. EDPS 2015. The European Data Protection Supervisor made it crystal clear that big data obtained through online tracking should still be considered personal even where anonymisation techniques have been applied. The reason is simple. It is easy infer a person's identity by combining allegedly 'anonymous' data with publicly available information from social media.

[53] EDSP 2015, p. 7

[54] Commission Communication "On Online Platforms and the Digital Single Market – Opportunities and Challenges for Europe", {SWD (2016) 172 final}, *COM (2016) 288 final*, Brussels, 25.5.2016 (Commission Communication 2016).

[55] JRC/IPTS Digital Economy Working Paper "An economic policy perspective on online platforms", 2016 (Digital Economy Paper 2016).

## 2.3 Control of big data contracts?

If the data protection authority in a Member State would have a right to verify the contents of the DTA and impose changes and perform checks on purpose limitations and accountability, this could create more trust and control. But first, the stakeholders in figure 2:

(1) Users of digital platforms – even if the personal information they supply may not always be personal data;

(2) Service providers on the digital platforms – whose business models may still be built on free access against data use;

(3) Big data analytics companies, who take data, use AI to enrich them and provide them as a paid service to other the service provider or third parties, and

(4) Clients who want to use the output of the analysis for scientific, medical, statistical and many more (some not very altruistic) purposes, want to know whether they own the data and for that, these data must be delineated. Figure 2 attempts to illustrate some of the dichotomies.

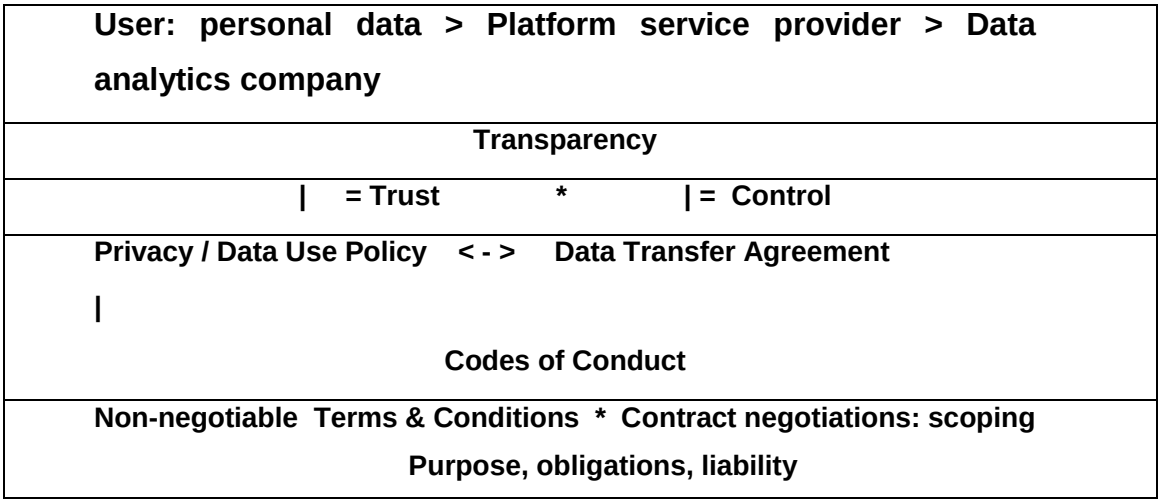



**Figure 2 Regulatory Compliance and contracts for big data**

Perhaps the debate should focus on whether, and if so, how data can qualify as a species of property. This could lead to delineating who owns them and what rights can be exercised. Especially in the United States, there seems to be quite a lot of opposition to "*mix property concepts with privacy concepts.*"[56] Even though personal data protection undeniably seeps through in commercial big data analytics, would the academic debate be better off by not just

[56] W. McGeveran, "Big data and privacy: making ends meet", *Conference Paper*, 2012 (W. McGeveran 2012).

looking at big data analytics from a trust and control perspective, but also from an economical contract law perspective? Rather than verifying whether private law functions as a control mechanism for enforcing regulatory requirements, big data could be approached from the perspective of property and contract law.

# 3. QUALIFYING (BIG) DATA AS PROPERTY & OWNERSHIP

## 3.1 Law of Property Notions

If a user *owns* her personal information, would that entail that she can do whatever she desires with the data? Could ownership function as a lever on giving consent to platform providers? If a client instructs a large and expensive big data analytics project, should it have all the freedom to keep the output exclusively for its own purposes?

Western legal systems are founded on the notion of property ownership, or law of property. Data can be anything, from files to location or traffic data, to IP addresses, log files, credit card files, or search terms; they can be digitized music, images or words. Data as such is an abstract notion: one cannot hold data in her hands. One cannot really give data as a present – for these purposes a durable data carrier would be required. In a world where data are mostly digital, the distinction between digital data and their storage – on which business cases are also built – and the underlying information characteristics at the basis of the database blurs more and more. It seems that using output of data analytics commissioned by companies blurs the fundamental right to privacy. Thus, an undesirable lack of nexus in the treatment and qualification of data in the context of personal data protection and the treatment and qualification of the same in the context of their economic value occurs.

Before going into ordinary property law, the intellectual property approach to data will be discussed.[57] The requirements for intellectual property protection – a form of originality – may turn out to be an unsurmountable obstacle when it concerns enormous collections of data that may have been enhanced by algorithms. Let it be reiterated that this Paper is concerned with ownership by private users who also provide the underlying data; yet, it is very unlikely that such data qualify as intellectual property rights. Bringing private users data ownership under the scope of intellectual property rights would require the defunct *sui generis* debate to rise again like a phoenix.

[57] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 59-110.

This paper does not focus on the issue of whether or not data should or could be 'owned' by the digital platform providers (or any other company, for that matter). Clearly, there is a pragmatic, but misty approach to data assembled by platform providers; and the Commissioner in charge of consumer rights is promising action to make the business models of platform provider more transparent in their general terms and conditions. This approach will be further explored below in this chapter and in chapter 4.[58]

There are pros and cons for "allowing" data to qualify as property. The justification for qualifying data as property is simple legal pragmatism, aligning economic hopes with private law measures. This combination, with a dash of regulatory invention on abuse of data that are personal makes a case for bringing personal information in the realm of 'ordinary' property law. The same for the output. What are the legal hurdles from a private law perspective? Bear in mind first the dichotomy between the (other) fundamental right of freedom of information and expression, which is often (ab-)used by proponents of free data use. But, as our society's digitization is quickly becoming irreversible, and where data protection regulation does not provide full protection of digital data floating around outside the control of the private users/data subjects, a new approach to data use may become inevitable.[59] The fact that the Commission has an eye for data processing rights in the context of intellectual property rights does not really clarify how data could be qualified. Indeed, the formulation in the Proposal on Copyright in de DSM turned the notion on its head: text and data mining of copyrightable material was to become a mandatory exception to the copyright ownership – in the context of temporary reproduction acts.[60] This upside-

[58] See Commissioner Vera Jourová, European Commission – *Press Release*, "Facebook changes its terms and clarify its use of data for consumers following discussions with the European Commission and consumer authorities", Brussels, 9 April 2019 (Commission/Facebook Press Release 2019); and "Facebook promises more openness after an intervention by ACM", *Het Financieele Dagblad* 10 April 2019, (translated from www.acm.nl/nl/publicaties/facebook-past-voorwaarden-aan-het-voordeel-van-consumenten, www.acm.nl/nl/publicaties/facebook-past-voorwaarden-aan-het-voordeel-van-consumenten: ACM is the Netherlands Competition Authority).

[59] For other perspectives see, *i.a.*, Determann 2019; H. Richter, P.R. Slowinski, The Data Sharing Economy: on the Emergence of New Intermediaries, *ICC International Review of Intellectual Property and Competition Law*, Vol. 50, Issue 1, pp. 4–29, January 2019 (Richter, Slowinski 2019).

[60] The EU Directive on Copyright in the Digital Single Market, COM 2016 (593) final (at the time of closing, it was still not final), which amends both the EU Copyright Directive of 2001 (2001/29/EC) and the Database Directive (96/9/EC).

down definition is not helpful.[61] The notion of intellectual property or *sui generis* rights focused primarily on rights for parties who invested in building databases. This was not only about databases, but went further, in terms of (1) maintaining and (2) exploiting the data.[62] It does not match with the current practices on digital platforms. The EU Database Directive has proven to be unsustainable. It did not address the existence of an underlying right on the actual data in detail.[63] Neither the main protection mechanism – copyright – nor the *sui generis* right, which was dead on arrival – a form of investment protection that does not extend to the data – award a clear and sustainable right for the party which considers itself the owner of data or big data. The Trade Secrets Directive added to the argument that (business) data should be treated as property.[64] It was intended to complement the intellectual property rights regime. The notion of trade secrets could perhaps and to some extent be applied to commercially valuable data and information that do not qualify for intellectual property protection. As such, the protection could be akin to the *sui generis* protection afforded under the database directive, if not for the fact that the object of protection there is a database. However, the key requirement is that the data are kept secret and as such, the party that controls those commercial secrets is required to undertake

[61] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 72-75.

[62] Think of (1) updating and adding new elements, data enrichment, applying hardware and tools not only to store but also to unlock data assembled and providing for safe carriers; and (2) exploitation of data would include granting user licenses to third parties, transferring data for money, or data as currency.
See, e,g., B. Van Asbroeck, J. Debussche, J. César, "Building the European Data Economy, Data Ownership, A new EU right in data", *White Paper*, Bird & Bird, 1 January 2017 (B. Van Asbroeck, J. Debussche, J. César 2017-1), p. 17-26. (E. Tjong Tjin Tai, "Data and the law of property", *WPNR: Weekblad voor Privaatrecht, Notariaat en Registatie* [in Dutch], 149 (7085), 993-998, 2015 (Tjong Tjin Tai 2015), p. 994*ff*. See also the English submission by E. Tjong Tjin Tai, "Data ownership and consumer protection," *Tilburg Private Law Working Paper Series*, No. 09/2017.

[63] **Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases,** *OJ L 77,* 27.3.1996*,* p. 20–28 (Database Directive 1996). The Directive created a new exclusive "sui generis" right for database producers, valid for 15 years, to protect their investment of time, money and effort, irrespective of whether the database is in itself innovative ("non-original" databases). The Directive harmonised also copyright law applicable to the structure and arrangement of the contents of databases ("original" databases). The Directive's provisions apply to both analogue and digital databases.

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

reasonable steps to protect the secrecy.[65] Once the data have been analysed and are published as big data, there is no trade secret anymore. Hence, I do not think that a trade secrets approach to big data would yield any functional result either. That brings us to private law notions of data as property.

## 3.2 Data property law?

Setting aside possible intellectual property and *sui generis* rights qualifications, it is not that easy to imagine the legal qualification of the commercializing of data under private law. For instance: how to put a mortgage on data – it is not that easy to calculate the economic value. Moreover, even though data can be easily reproduced and retransmitted,[66] is it relevant to determine who qualifies as the first 'owner' of the data, especially in light of how the data of the private user were collected.[67] Probably as a consequence of legislators having cold feet in addressing this fundamental question, there is no EU or Member State's approach to the qualification of data as property in some form. In legal practice there is some case law,[68] and there have been ongoing scholarly debates on the data property issue.[69] As displayed in the data policies cited above, the gap between the two notions on data – privacy protection versus ownership – is underlined by the sad reality of many controllers issuing privacy and data policies that are hollow in terms of providing protection to the data subject and conveniently vague in terms of what the controller may do with the personal data it assembles – often without getting prior approval on *a case by case* basis from the data subject. Ownership of data by private users could remain fiction. Yet, the fact that there is no EU regulation that qualifies the legal status of data under property law does not prevent the Commission from voicing that – next to the protection of personal data – data ownership is a hot topic for regulation. This debate would most likely extend to data ownership by corporations, especially platform providers. However, the current context seems to be out of focus. The Commission focuses on data property solely as being an internal market issue.

[65] See Article 2 Trade Secrets Directive.
[66] So can software, but if satisfying the originality criterion, and subject to the exclusions and exhaustion doctrine, software will fall under the protection regime.
[67] *Cf.* Tjong Tjin Tai 2019, p. 10ff.
[68] An early and not entirely convincing example can be found in a decision of the upper court of Karlsruhe going back to 1995 and that related to the destruction of data: OLG Karlsruhe, Urt. v. 07.11.1995 – 3 U 15/95 – *Haftung für Zerstörung von Computerdaten.*
[69] *Cf.* B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 17 and p. 22-25.

Yet, the Commission acknowledges that there may be a regulatory gap that could cause harm:[70]

> "*Barriers to the free flow of data are caused by the legal uncertainty surrounding the emerging issues on 'data ownership' or control, (re)usability and access to/transfer of data and liability arising from the use of data*."[71]

The scope of information is the basis for the processing. It is that basis that may or may not be qualified as an absolute property right.[72] In my view, the Commission urgently needs to formulate a policy on establishing data ownership. Where the harmonization of private law in the EU remains a taboo, could there be room for zero base harmonization now that the Member States do not appear to have clear visions on if, and if so, how to qualify the legal status of (big) data in there civil codes? Conceptual problems appear to abound. A problem is that property is any interest in an object, tangible or intangible, that is directed against everybody (the *erga omnes* effect).[73] Exercising control over one's 'own' data is something different from 'owning one's data.'[74] The *erga omnes* effect may be aimed at certain stakeholders only and, thus, less effective. The second problem is that, without a proper qualification of the nature data (para. 3.1), contract law would support probably only *the way in which* the data might be exploited. This writer is not very impressed by the top down approach: definitions of ownership to determine whether data can be property. Ownership should be the result of there being a property; not the other way around. A third problem is that in privacy law, control is a term does not apply solely to a data subject. Linguistically, control applies to data processing by the controller. Under private law, control must also be exercised in the data subject's realm. Control should not be restricted to the digital platform provider or the client's use of the platform. The fourth problem is that legislation in civil law

[70] Commission Communication on Towards a Thriving Data-Driven Economy, COM (2014) 442 final.

[71] Commission, "European Free Flow of Data Initiative within the Digital Single Market" (Inception impact assessment, 2016) <http://ec.europa.eu/smartregulation/roadmaps/docs/2016_cnect_001_free_flow_data_en.pdf>

[72] Compare the French Code Civil, article 544: "*La propriété est le droit de jouir et disposer des choses de la manière la plus absolue (…).*"

[73] See N. Purtova, 2011, for a theoretical discussion of property rights in personal data (Purtoya 2011).

[74] Other than that the GDPR considers it a desirable trait: see recital (7): "*Natural persons should have control of their own personal data*," and: "*Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.*"

countries and case law in common law countries considers property law as a closed system. It not easy to define a new type of good under property law, be it personal information or the outcome of a data analysis. Courts in common law countries have offered an opening to property law being more of restricted system than a closed system:

> "*Before a right or an interest can be admitted into the category of property, it must be (i) definable, (ii) identifiable by third parties and (iii) have some degree of permanence or stability*."[75]

It appears that the third requirement will not be satisfied easily on a digital platform. Consider the case of online tracking of information on social media: beyond the ownership question lies the question whether the personal data that are being mined are more of a fleeting, or of a stable presence. But, this should not be an insurmountable problem. Most data are stored on a stable carrier – and that includes, in my opinion, data in the cloud. Once this obstacle is overcome, there is the need to bring data into a defined category of property. Examples are movable and immovable property; material and immaterial property; tangible and intangible property. The negative starting point is that data cannot be considered goods, since – without a carrier – data are not capable of materiality. In common law, some scholars have opined on the need to treat data as a proprietary law issue. Property is often defined as "a bundle" of rights and obligations rather than emphasizing the materiality. This approach makes sense.[76] The data carries the economic value, not the data carrier or database. Without the data these carriers are empty shells:

> "*That is to say that the protection of the economic value inherent in personal information should be grounded in property rights acknowledged by the law*."[77]

A further theoretical problem regarding the qualification of data under private law is that it would be difficult for the owner to warrant exclusivity of the data and the database – data can be copied easily and infinitely as was established above. Besides the fact that this argument was used in the discussion of the protection of software – and was overcome – the fact that the owner can make the data available to many different processors or users does not stand

[75] Judgement in National Provincial Bank v Ainsworth [1965], AC 1248, opinion by Lord Wilberforce, cited in C. Rees (2014), p. 77.
[76] Tjong Tjin Tai 2015, p. 995, who refers to G.S. Alexander, E.M. Peñalver, *An Introduction to Property Theory,* Cambridge: Cambridge University Press 2012 (G.S. Alexander, E.M. Peñalver 2012).
[77] Rees 2014, p. 2.

in the way of establishing it as a property. Developments in the exploitation of big data, their manageability by different stakeholders simply require a functional approach: data are, at the least, comparable to goods.

The pragmatic approach to the qualification of data as property perhaps also requires answering what private law aspects matter in data ownership. First, the right of use; second a form of control exclusivity of the party who exploits the data; third, the right to dispose of the data; and fourth, rights and obligations that may be attached to the data, e.g., the possibility of liability for their content, or the right to claim the ownership of data that are in the possession of a third party.[78] There is also the question of enforcement of data ownership. Art. 79 GDPR contains a choice of forum to facilitate data subjects to enforce their rights under the GDPR.[79] Perhaps private law should not simply complement the enforcement of data protection law. Neither should data protection law supplement private law. Both data protection regulation and private law have in common that they aim at embedding trust and control of data. The regulatory gap that may arise is the result of is the result of overlapping, mixing or exclusionary administrative law and private/consumer law rights and obligations and a lack of transparency regarding their use. Private users are served by overlapping, complementary rules; not by discussions regarding competences, or different interpretations of material legal provisions.

## 3.3 Exercising data ownership under data protection and private law

The starting point for embedding personal information in property law contracts should not merely consist of a replication of the models for protection of personal data under the GDPR and related legislation and regulation.[80] A different approach, notably, focused on the enforcement of rights present in the GDPR, may be wise. As was seen, in terms of big data analytics agreement between the controller and a third party, the policies leave much to be desired, and the private users' rights under the GDPR must be enforced still by regulatory authorities.[81]

[78] For a bottom-up approach to personal information as a case study for property law, see J. B. Baron, "Property as Control: The Case of Information", 18 *Mich. Telecomm. Tech. L. Rev*. 367 (2012) (J.B. Baron 2012).
[79] *Supra*, para. 2.
[80] B.J. Evans, "Much Ado About Data Ownership", 25 *Harv. J.L. & Tech* 69, 2011 – in the context of patients' privacy protection.
[81] Supra, para. 2.1.

This stows liability claims far away. Some scholars – in the US – distinguish between rules on property, and rules on liability – without addressing whether this is a matter of law or contract.[82] Or, as Lessig clarifies:

> "*The key to a property regime is to give control, and power, to the person holding the property right.*"[83]

I support the position to look at the exercise of ownership first: what rights would accompany the property?[84] The exercise of exclusive rights over the data property would fall into: rights which are exercisable in personal information against everybody *(rights in rem*, i.e, rights that are associated with a property and not with a personal relationship) and more limited: rights *in personam*, (i.e., rights which are attached to one's persona). Rees writes:[85]

> *"The ownership paradigm will encourage the use of privacy enhancing technologies and state of the art security measures to protect data. Those who hold vast quantities of personal information will realise the risks inherent in losing the property of vast numbers of third parties and the risk of consequent class actions for damages for having done so."*

It is an open question whether ownership should have the nature of an exclusive or a non-exclusive right. This requires further scholarly debate on the intersection between property law and the desire to stimulate through regulation the European data economy. The complication in defining ownership lies in the fact that, in practice, different third parties and the algorithms or other analytical tools they apply, may be involved in various stages of the data analytics process. This creates an extra issue that is best avoided: agents or subcontractors claiming big data (joint) ownership. It would make economic exploitation of the data more difficult and the legal standing of the private user weaker. Under property law – joint ownership is likely to create legal issues as regards the exercise of exploitation rights and the enforcement of data ownership rights. A possible solution for this is provided in the Data Ownership White Paper. The solution entails imposing a "traceability obligation" on the transferee who engages in the big data processing.[86] In practice, this obligation would entail that the transferee must keep logs of all steps in data processing for the performance of data

[82] G. Calabresi, D. Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral", 85 *Harv L. Rev.* 1089 (1972).
[83] L. Lessig, *Code and Other Laws of Cyberspace* 160 (1999).
[84] C. Rees 2014, p. 78.
[85] C. Rees 2014, p. 79.
[86] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 125-126.

analytics. Or: which party has done what with the data, what did their efforts result in, and, thus, why are they the owners? Still, once we are willing to agree that data ownership as a legal concept would serve to support both trust of the data user in the processing of its personal data and control by the service provider in data transfer agreements, we face another legal question: how to ensure that the two-step transfer approach creates trust when there are *hundreds of thousands* owners party to one agreement? *Prima facie*, it seems that the practical way forward would be to give the platform provider a form of proxy to negotiate the terms of the data transfer agreement on behalf of the data subjects. But, that requires trust in that provider.

The qualification of (big) data under private property law notions may be an unresolved matter that requires further extensive legal research. Notwithstanding this need for research, some academics, including this writer, argue in favour of a functional and more open approach to exercising control and trust over data that have been either offered or generated by private users/data subjects. Consequently, a more detailed perception of private law options to exercise ownership rights should be (re-)considered. In this approach, consumer law notions barge in.

## 3.4 Contractual regulation of big data analytics & consumer rights

It can be inferred from the brief discussion of the legal qualification of data that contractual embedment of what the data are and how they may be processed fairly, is part of necessary functional approach to protect rights both of the party who desires to transfer data ownership (transferor) to another party (transferee) pursuant to a fair contract and any data subjects at the source of the transfer. There should be freedom of contract to negotiate the terms of a DTA. But this freedom is delineated by regulatory concerns, such as concerning transparency of the processing.[87] A DTA should begin with specifying the scope of the property rights in data attached to the transfer and the purposes for the transfer.[88] This qualification requires prior legal analysis as to what data input must be provided to the data analytics company (akin to a Privacy Impact Analysis). Subsequently, it is key to define what

[87] N. Helberger, F. Zuiderveen Borgesis, A. Reyna 2017, p. 1430*ff*.

[88] This Paper does not deal with possible data license agreements, based on copyright or database rights in the source data. If have explained above that I am not convinced that an intellectual property rights approach to data will be functional. For an extensive discussion of IP rights in the source data and their implementation in a form of license agreement: B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 59-78 on copyright and p. 82-105 on the exploitation of *sui generis* rights in databases.

the conditions attached to the transfer are. They can be as broad or as limited as the transferor decides, provided that it takes into account prior rights. These would probably entail personal data that have been masked.

By using a DTA the transferor(s) of the data can delineate what can and cannot be done by the transferee. Whether the transferee acquires a form of ownership in big data produced is also a matter of contract discussion. As is the case with a license agreement, the scope of use can be as limited or as extensive, as the parties agree. The scope is dependent upon the activities to be undertaken by the transferee and whether the cooperation between transferor and transferee qualifies as a service or more a cooperation agreement. Conversely, the transferee wants to delineate what it can do with data transferred to it. Possible scope of use and purpose could include the right to aggregate, reproduces, modify, mask, filter, enrich, combine, merge or partition data. Whether the transferee is entitled to share, make public, outsource parts of the data or even delete the data must be considered carefully by the transferor.

For at least two reasons, it is important that the DTA contains provisions on rights for the transferor to: (1) audit and inspect what the transferee does in terms of processing the data, (2) govern and control the manners in which data are processed, and for what purposes and (3) ensure accountability by the transferee:

- The personal data regulation requires this; and
- The transferor – whether it considered as a controller of the data or not, needs to have an insight in what the transferee does for reasons of being able to enforce by contracts its own rights and the rights of private users/data subjects.

Embedding privacy by design in the development and application of big data analytics projects is a great example of convergence of market regulation and private law. Including contractual obligations such as regarding the implementing technical and organisational measures to address matters including data security, data minimisation and data segregation makes the obligations better enforceable.

Turning now to consumer law protection, the first point to be made is that its rationale is linked less to the protection of fundamental rights.[89] But to what extent is that a hurdle? Isn't the whole point of bringing in consumer law requirements that the private users may directly obtain a legal remedy from the digital platform provider who uses their (non-personal) data in a manner that is inconsistent with either the scope of use on their platform, a *Schutznorm* – such as the protection of personal data – or its own general terms and conditions (including

[89] N. Helberger, F. Zuiderveen Borgesis, A. Reyna 2017, p. 1435.

its privacy policies). Isn't one of the advantages of bringing in consumer law that unfair contract terms could be null and void, or voidable? Granted, this requires further thinking on what could constitute unfair contract terms relating to the use of data of private users/consumers (who, in all likelihood also are data subjects). No matter that the legal subject may be one and the same person, if the political goal is to empower private users on digital platforms to get more control over and have more trust in the data that are traceable to them or their personal data, then this should be done bottoms-up from a consumer law perspective. There is nothing – other than perhaps a partial duplication of efforts that stands in the way of this approach. The GDPR contains a solution regarding locus and basic rights in art. 79 – against enabling consumers to go either one or both ways, when their data are compromised. The consumer approach to big data analytics contracts is in its infancy or, at best, a work in progress. The notions that need to be explored further from a private law perspective are proportionality of the contract provisions and specific transparency obligations. Digital platforms are required to use **clear and easily accessible** terms and conditions of their online intermediation services. For instance, they should provide a **statement of reasons** each time they decide to suspend or terminate the use of their services by a business user. It is exactly this kind of behavior that may contribute to the private users having more control over the data use and more trust in the digital platform providers. Embedding these legal obligations in general terms and conditions appears to me as a very effective measure

The principle of transparency – or information provision – often used in EU internal market regulation, could prove to be a palpable solution for private users on digital platforms. The draft Online Intermediary Services Regulation[90] presents a few meaningful obligations that could be imposed also on the big data analytics providers either directly or indirectly through the digital platform providers. The Proposal provides for a **transparency**

[90] Still under construction at the time of closing this paper and not to be confused with the draft Digital Content Directive from 2015; see: Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content COM(2015)634 final, referred to by N. Helberger, F. Zuiderveen Borgesius, A.Reyna 2017, has not passed the legislative process yet. By January 2019, the Commission mentioned that a political compromise (which seems to grant a bit more protection to the suppliers, i.e., digital platform providers). had been reached.

**requirement.** Digital platforms providers are required to use ***clear and easily accessible*** terms and conditions of their online intermediation services.[91]

Providing transparency on the use of data – or their part in the business model of the platform provider is exactly the kind of behavior that may contribute to the private users having more control over the data use and more trust in the digital platform providers.[92] Embedding these legal obligations in general terms and conditions appears to me as, potentially, a very effective measure. The private user could have better recourse against the digital platform provider. The explanatory note mentions that the main goal of the regulation is to establish a legal framework that guarantees, in the first instance, **transparent terms and conditions** for business (and private it seems) users of online intermediation services. Business users are then also guaranteed, within this framework, effective possibilities for **redress** when these terms and conditions are not respected.

But still… there continues to be a lack of harmonization of European contract law; see, *e.g.*, the 2011 Consumer Rights Directive, which contained very few personal data-related provisions benefitting consumers.[93] Probably, meaningful protection provisions could be copied from the Unfair Commercial Practices Directive.[94] The starting provision would be the obligation to provide consumers with information about the collection and commercial exploitation of personal data.[95] That is a nice start. Misleading or false information, as in the CA case, would be considered an unfair commercial practice should lead to a sanction. A nice example is the description of a digital services as being free of charge in the context of the (re-) use or transfer of their personal data.[96] Perhaps a reconsideration of the Unfair

[91] For instance, they should provide a **statement of reasons** each time they decide to suspend or terminate the use of their services by a business user.

[92] And there is a current trend, see the Commission/Facebook Press Release 2019.

[93] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (Consumer Rights Directive), 2011/83/EU; see also the commentary in *Concise European Data Protection, E-Commerce and IT Law*, S. Gijrath, S. van der Hof, A.R. Lodder, G-J Zwenne, eds., 3rd edition, Kluwer Law International, Alphen aan de Rijn, 2018.

[94] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive), OJ 2005, L. 149.

[95] See also art. 6 Unfair Commercial Practices Directive.

[96] This would be a misleading omission. See also N. Helberger, F. Zuiderveen Borgesius, A.Reyna 2017, p. 1443.

Contract Terms Directive could be useful as well. At the high level, the directive introduced the notion of "good faith" to prevent imbalances in the rights and obligations of consumers on the one hand and sellers and suppliers on the other hand.[97] Besides, the Unfair Contract Terms Directive includes the blue list with terms that could be considered unreasonable.[98] These terms could be enhanced or supplemented in this Directive or another EU instrument to include better terms on the (re-) use of a private user's data, including transfer thereof as well on transparency in terms of how there are treated in the context, for instance, of 'free services'.[99] Clearly, the digital platform provider would have to make it clear from the beginning that the free of charge services require the use of data of the private user as a counter-performance. Not only this mere fact, but also the scope of use could be a supplementary term, although some of the relevant provisions in the GDPR could be incorporated in the unfair contract terms as well. What would be the consequence of non-transparent or incomplete contract terms on data use, and transfer? Such unfair contract terms are not binding for consumers. Moreover, the Directive also requires contract terms to be drafted in plain and intelligible language. As a consequence, ambiguities would be interpreted always in favor of consumers. This obligation could serve as a lever against opaque, incomplete or misleading provisions on the commercial exploitation of a private user's (personal) data, whether they represent a value or not.

In my view, consumer law protection provisions could function as a meaningful instrument to empower the private users in exercising their personal data rights in contracts with digital platform providers. And the scope could be improved by offering more clarity as to the manner in which the private users' data are valued and reused. After a round of consumer empowerment, some nuance is necessary. A purely contractual approach brings issues of its own.[100] Let me remind the reader of the problems with scoping property in data transfer agreements.[101] Private law incorporates the notion of third party beneficiary rights. That

[97] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts as amended, *OJ L 95, 21.4.1993, p. 29–34.*

[98] Terms Referred to in Article 3 (3) of the Unfair Contract Terms Directive.

[99] *Cf*. A. Metzger, "Data as counter-performance: what rights and duties do parties have?". 8 Journal of Intellectual Property, Information Technology and E-Commerce Law (2017), p. 2-8 (Metzger 2017). See also, more extensively: N. Helberger, F. Zuiderveen Borgesius, A. Reyna 2017, p. 1442-1449.

[100] See on the somewhat complicated application of article 5(1) Consumer Rights Directive, N. Helberger, F. Zuiderveen Borgesius, A.Reyna 2017, p. 1444*ff*.

[101] B. Van Asbroeck, J. Debussche, J. César 2017-1, p. 5, conclude that "(…) such situation is not sustainable in a data-driven economy and with the fast-increasing development and adoption of data mining and analysis tools."

would entail that the transferor should require from the transferee to include provisions in the DTA or in the contract with the digital platform provider to protect the personal data of the data subjects and that it should commit to certain contractual standards. In practice, that appears hard to achieve, especially since the data subjects – often consumers, who sometimes are willing to grant access to their personal data in exchange of information or a price discount – have no standing in the actual negotiations. General terms and conditions are as little negotiable as privacy policies. But if the FCO Ruling stands in appeal, that could entail a meaningful improvement to the private users' legal positions.[102]

Enforcing contractual accountability arrangements may prove to be difficult where the transferee/processor employs subcontractors or other third parties and fails to secure adequate obligations from these parties; and where the transferor will experience difficulties in contract enforcement of data subjects' interests by way of third party beneficiary rights. Other problems with contracts will be the scope of safeguarding information and data security and delineating contractual liability. An example is the liability for loss, destruction or damage to data – in many standard IT contracts, contractual liability of the service provider for these kinds of events in often excluded.

Finally, does the fact that the data subjects have little say on the transfer of their – depersonalized personal data – to a third party big data analytics company imply that there is a (stronger) duty of care on the transferee to safeguard their privacy? An option that the Commission considers is issuing model contract terms, codes of conduct and/or default contract rules; along with a right to access for "public interest" and scientific purposes. It certainly does not appear impossible or impractical to further investigate how a DTA can impose both contractual and regulatory requirements; it just requires an open mind as to how to align personal data protection with private law to achieve a better result. It might engage data subjects more in the potential use risks *and* opportunities of big data analytics. Defining ownership rights and scoping in DTA's may also make the enforcement of competition law better manageable. The competition authorities will have a sound basis to start their investigation on.[103]

## 3.5 Interim conclusion

[102] See, *infra,* para. 1.1.

[103] I will not discuss these same characteristics as an argument against having well written and detailed DTAs.

In sum, a functional approach to consumer law and data protection is likely to yield better results for private users in terms of controlling and monitoring what happens with the (non-personal and personal) data they hand over to the digital platform, consciously or not.

## 3.6 (Extra-contractual )liability for data (mis-)use?

Probably, an extra strong case for aligning private law with personal data regulation is liability for damages. If the legal qualification for data is complex and has not been fruitful in defining the rights and obligations of the parties involved both under property and contracts law, then what can be said about prospective contractual – or extra-contractual – liability for data? First, it would be helpful to determine in the DTA what damage causing events could occur, when a party who either 'owns' or transfers the data to a third party, and the data are either (1) lost, destroyed, garbled, damaged, (2) manipulated, modified, abused, falsified, (3) transferred to one or more other parties, (re-)sold, or (4) published, made available to others? Second, before addressing which party would be liable, the damage causing events need to be tied to actors. Third, it is not sufficient to rely on general legislation regarding extra-contractual liability, for instance, risk liability. This requires a whole separate legal analysis of the law and the differences on liability legislation across the Union.

There is an instance where the EU already brought together a breach of community law and private law damage claims: the 2014 Directive on damages.[104] There are some fairly clear legal provisions in the GDPR on liability for damages suffered as a result of misuse of personal data. This "*Schutznorm*" may support private parties' claims. Article 82 GDPR provides that any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.[105] This norm then needs to be transferred to the data analytics service providers, and the clients. The wording in the GDPR is broad and

[104] Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, *OJ* L 349/1.

[105] A processor shall be liable for the damage caused by processing *only* where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. See also sections 3 and 4 of Article 82 GDPR. Section 3 provides that a controller or processor may exempt itself from liability if it proves that it is not in any way responsible for the event giving rise to the damage. Section 4 is the well-known provision establishing joint liability.

concrete for data controllers and data processors to include liability provisions in their processing and big data analytics agreements. Recital (146) to the GDPR speaks for itself (emphasis added) and I will cite the elements that are relevant in terms of establishing liability – first, the scope:

> "(…) *Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation."*

Second, the rights of the data subjects are set out:

> *"Data subjects should receive full and effective compensation for the damage they have suffered."*

Article 28, subsection 4 GDPR bears particular relevance for a digital platform service provider who enters into a big data analytics contracts with a third party. It actually provides a duty to contract in a straightforward manner (emphasis added):

> "*Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations*."

The consideration cited above should be translated into liability for misuse of personal data by controllers and processors alike. And the limitation of liability clause should be reasonable and compliant with the terms of the GDPR. I hope this section offers support to liability being an area where regulation and private law agreements should come together.

## 4. BIG DATA ANALYTICS AGREEMENTS: FOLLOW-UP?

Let us briefly return to the CA/Facebook controversy. We are not certain whether the transfer of data was supported by an agreement between CA/Facebook. In light of the Data Policy cited under 1., we know that Facebook committed only to imposing heavy

confidentiality obligations on CA. Various regulatory authorities are investigating whether Facebook has complied with its regulatory obligations and, at a more general level, whether it has exercised a duty of care against CA. If they had, then this would entail that trust between the digital platforms provider and its users could be established. Much depends on whether and if so what kind of contractual obligations Facebook imposed on CA. A contractual assessment of the scope of the contractual relationship between Facebook and CA brings a host of questions, such as:

(1) How was big data ownership qualified in the DTA?
(2) Did Facebook in fact provide CA with "non-personally identifiable information" only; were personal data masked adequately?[106]
(3) What did the parties agree on the scope, depth, performance, veracity and control of the output (big data) of the data analytics – did Facebook have a say?
(4) Did Facebook negotiate and have right to control whether big data analysis on non-personal data was performed and was compliant with privacy regulation?
(5) What did the DTA provide on contractual liability of either party under the DTA? Did the DTA contain an indemnification from CA to Facebook?

These questions serve to underline that it is preferred to have a DTA than to rely on data protection or competition law enquiries that reveal that the transferor has not exercise due care from the start of the transaction. Digital platforms' regulation could then supplement the contract by requiring the digital platform service provider that wishes to enter into DTA's with third parties to contract in user rights. Additionally, regulation could oblige the transferor to safeguard third party beneficiary rights on behalf of the data subject against the transferee.[107]

# 5. FINAL REMARKS

## 5.1 Let's not forget the stakeholders

It is time that all stakeholders, recognize the gap that exists between: (1) extensive personal data protection regulation and competition law and (2) the lack of (harmonisation of) legislation and regulation that provides for qualification of data and their collection under

[106] See above under "Just another data policy."
[107] The EDPS considers that data portability helps competition and consumer protection, EDPS 2015, p. 13*ff*.

private law, including their use under unfair contract terms legislation. Property is a notion that is present in all (baring a few remaining communist regimes) legal regimes. There are scholars who argue for a pragmatic approach: data can be regulated in contracts without the need of qualification. Even in a restricted property regime, the preference should be to specifically grant a property right to personal information in private law. This will enhance both their economic use and the contractual enforcement of rights. In case personal information is recognized as a property right, then the legislation should provide the criteria for determining who owns the data.

If society wants data subjects to have the option to claim damages for misuse of their personal information or data, then it is helpful that a link is established with private law. Contractual arrangements regarding the onus of liability under any DTA may be subjected to scrutiny by NRA's or courts, when there is a serious breach of privacy rights of the data subject.[108] Only civil courts are competent to determine the basis for, the scope and amount of damages suffered by a data subject. The GDPR contains a "*Schutznorm*" which may determine extra contractual liability; however, the data protection authorities can impose fines, not damage compensation to private parties.

## 5.2 Back to the economic and trust factors

This writer argued that the data economy and the digital platforms policies by themselves are inadequate to regulate behaviour of parties who make money from analysing human behaviour. I made the point that service provider is the man in the middle, whether it acts as a controller or a processor. It is really up to the service provider to engage in setting the boundaries (the purpose limitation) with the data analytics company; and to survey contractual compliance.

If data are a resource, a commodity of their own, then affected parties are entitled to transparency on the transactions contemplated with their personal data. The Commission and other EU institutions are uncertain that the market for the trade in for personal information is transparent, fair and efficient. Contracts could alleviate these concerns.

'Sharing' data – as it were – in exchange of 'free services' is not desirable if the data subject does not have an indication of what its personal information might be used for and how much value is attached to that information and in which context. The digital platforms

[108] See again the GDPR, recital (146) on conflicting court rulings.

regulation should include standards to assure fair compensation to users who are willing to share their personal information.[109]

## Bibliography


[1] G.S. Alexander, E.M. Peñalver, *An Introduction to Property Theory,* Cambridge: Cambridge University Press 2012 (G.S. Alexander, E.M. Peñalver 2012).

[2] J. B. Baron, "Property as Control: The Case of Information", 18 *Mich. Telecomm. Tech. L. Rev*. 367 (2012) (J.B. Baron 2012).

[3] L. Bennet Moses, "How to Think about Law, Regulation and Technology, Problems with "Technology as a Regulatory Target", *Paper* http://dx.doi.org/10.5235/ 17579961.5.1.1. (L. Bennet Moses, 2013).

[4] M. Burri, M. Elsig, R. Polanco, R.Schär, S. Klotz, The Governance of Big Data in Trade Agreements: Design, Diffusion and Implications, work progress, University of Lucerne.

[5] M. Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation", *UC Davis Law Review*, Vol. 51, 2017, pp. 65-133 (M. Burri, 2017).

[6] G. Calabresi, D. Melamed, "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral", 85 *Harv L. Rev.* 1089 (1972).

[7] D. Geradin, "Ensuring sound regulatory processes: For a principled approach", *TILEC Dicussion Paper DP 2017-030*, ISSN 1572-4042 (D. Geradin, 2017).

[8] European Parliament, *Report*, "Legislative Train", 06.2017 (European Parliament 2017).

[9] I. Graef, M. Husovic, "Response to the Public Consultation on 'Building a European Data Economy', *TILEC Discussion Paper, DP 2017-016*, ISS 1572-4042, April 2017 (I. Graef, M. Husovic, 2017).

[10] I. Graef, M. Husovic, N. Purtova, "Data Portability and Data Control Lessons for an Emerging Concept in EU Law", *Tilburg Law School Legal Studies Research Paper Series*, No. 22/2017 (I. Graef, M. Husovic, N. Purtova 2017).

[11] M. Granieri, A. Renda, *Innovation Law and Policy in the European Union, Towards Horizon 2020*, Springer, 2012 (M. Granieri, A. Renda, 2012).

[12] W. McGeveran, "Big data and privacy: making ends meet", Conference Paper, 2012 W. McGeveran 2012).


[109] EDSP 2015, p. 12.

[13] A. Metzger, “Data as counter-performance: what rights and duties do parties have?”. 8 Journal of Intellectual Property, Information Technology and E-Commerce Law (2017), p. 2-8 (Metzger 2017).

[14] N. Helberger, F. Zuiderveen Borgesius and A. Reyna, “The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law”, *Common Market Law Review* 54: 1427-1466, Kluwer Law International, 2017 (Helberger, Zuiderveen Borgesius, Reyna, 2017).

[15] McKinsey Global Institute, Disruptive technologies: Advances that will transform life, business and the global economy, paper, May 2013 (McKinsey 2013).

[16] J. Modrall, “Big Data and Algorithms, focusing the discussion”, Oxford University, Business Law Blog, 15 January 2018 (J. Modrall 2018).

[17] OECD, *Big data: Bringing competition policy to the digital era*, 2016.

[18] J. Prufer, C. Schottmüller, “Competing with Big Data” (February 16, 2017). Tilburg Law School Research Paper No. 06/2017; TILEC Discussion Paper No. 2017-006; CentER Discussion Paper 2017-007, https://ssrn.com/abstract=2918726 (J. Prufer, C. Schottmüller, 2017).

[19] N. Purtova, *Property rights in personal data*: *a European Perspective*, thesis, University of Tilburg 2011 (N. Purtova, 2011).

[20] PWC, “Benefiting from big data, A new approach for the Telecom Industry”, *Report* 2013.

[21] K. Radha, B. Thirumala Rao, Shaik Masthan Babu, K. Thirupathi Rao, V. Krishna Reddy, P. Saikiran, “Service level agreements in cloud computing and big data”, *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 5, No. 1, February 2015, pp. 158~165.

[22] C. Rees, “Who Owns Our Data?” (2014) 30(1) Computer Law & Security Review 75 (C. Rees 2014).

[23] B. Schermer, “Privacy and property: do you really own your personal data?” *Weblog*, Leiden University, 15 September 2015.

[24] E. Tjong Tjin Tai, “Data and the law of property”, WPNR: Weekblad voor Privaatrecht, Notariaat en Registatie [in Dutch], 149 (7085), 2015, 993-998 (Tjong Tjin Tai 2015).

[25] E. Tjong Tjin Tai, “Data ownership and consumer protection,” *Tilburg Private Law Working Paper Series*, No. 09/2017.

[26] TNO, Ecorys, IVIR, *Digital Platforms: an analytical framework for identifying and evaluating policy options*, Report, Ministry of Economic Affairs, the Netherlands, 2015.

[27] B. Van Asbroeck, J. Debussche, J. César, “Building the European Data Economy, Data Ownership, A new EU right in data”, *White Paper*, Bird & Bird, 1 January 2017 (B. Van Asbroeck, J. Debussche, J. César, 2017-1).

[28] B. Van Asbroeck, J. Debussche, J. César, “Data Ownership, A new EU right in data”, *Supplementary Paper*, Bird & Bird, 31 March 2017 (B. Van Asbroeck, J. Debussche, J. César, 2017-2).

[29] B. van der Sloot, S. van Schendel, “Ten Questions for Future Regulation of Big Data, A Comparative and Empirical Legal Study”, 7 (2016) JIPITEC 110 par.1. (B. van der Sloot, S. van Schendel, 2016).

[30] H.U. Vrabec, Uncontrollable Data Subject Rights and the Data-driven Economy, dissertation, University Leiden, 2019 (Vrabec 2019).