



Universiteit
Leiden
The Netherlands

Uncontrollable: Data subject rights and the data-driven economy

Ursic, H.

Citation

Ursic, H. (2019, February 7). *Uncontrollable: Data subject rights and the data-driven economy*. Retrieved from <https://hdl.handle.net/1887/68574>

Version: Not Applicable (or Unknown)

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/68574>

Note: To cite this publication please use the final published version (if applicable).

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/68574> holds various files of this Leiden University dissertation.

Author: Ursic, H.

Title: Uncontrollable: Data subject rights and the data-driven economy

Issue Date: 2019-02-07

4. CONTROL AS A CENTRAL NOTION IN THE DISCUSSION ON DATA SUBJECT RIGHTS

4.1. Introduction

Chapter 2 presented four values that are critical for individual well-being but can be undermined as a result of ubiquitous personal data collection, mining, and processing in the data-driven economy: *autonomy, privacy, transparency, and (market-)power symmetry*. As shown in the present chapter, one common denominator of all four values is the concept of *control over data*. The individual control over data is most directly reflected in the value of autonomy as an expression of individuals' self-determination and free will. Privacy, in particular informational privacy, also overlaps with the concept of (individual) control, especially when it is defined as the right to determine the use of personal information and flows – in other words, privacy as control over personal information.⁵¹⁵ Transparency is a necessary precondition for control, whereas power asymmetries grow out of imbalanced control distribution.

Chapter 2 also indicated that individuals' control in the data-driven economy is rather weak and some other groups of actors are in a considerably better position to exercise control over personal data. The data-driven economy has generated an environment in which the so-called data barons (i.e. large companies, government agencies, intermediaries) have a unique control over digital information, which is no longer counter-balanced by the control of other actors.⁵¹⁶ As was explained in Chapter 3, data protection law looks at data barons as data controllers. As the name indicates, controllers have the measures and power to control data. To prevent abuses, the law constrains their powers and imposes data protection duties. The unequal distribution of control among the actors in the data economy is further addressed by the GDPR provisions that aim to enhance data subjects' control. Chapter 3 highlighted two sets of data protection rules in the GDPR: those on consent and those on data subject rights.

Besides data subjects and controllers, there is a third group of actors also capable of exercising control over personal data use. This group is composed of data protection authorities and some other public bodies.⁵¹⁷ Some argue that the rigour of control that they exercise should increase in the upcoming years.⁵¹⁸ Namely, in the data-driven economy, data protection authorities rather than users have the technological knowledge to evaluate the risks of data processing and the access to adequate measures.⁵¹⁹

Control appears to be a central notion for the discussion on data subject rights, but in data protection law it is poorly articulated. Before specific rights are analysed, the notion of control must be explored in more detail. To this end, the research sub-question addressed in this chapter is the following: *What does the notion of individual control entail and, specifically, how does it relate to the discussion on data subject rights?* (the third research question) By answering this question, this chapter serves as a

⁵¹⁵ Solove (2004) 77; Westin (2015).

⁵¹⁶ Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-Thinking The "notice and Consent" paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law and Security Review 643, 650.

⁵¹⁷ E.g. consumer protection authorities.

⁵¹⁸ Hijmans (2016) 497; Mantelero (2014) 657.

⁵¹⁹ Ibid., 647.

bridging section between the general part on the economic reality of the data-driven markets, and the more specific part on data subject control rights. The discussion on the notion of control is key to understanding the role of control rights in the data-driven economy and therefore serves as a basis for answering the key research question of this thesis.

The chapter is organised as follows. Section 4.2. analyses the notion of control by summarising how different scientific disciplines interpret it. Section 4.3. then explains what role the concept of control plays in the area of human and fundamental rights protection. Four fundamental rights that embody ideas of control are briefly explained: the right to property as the most apparent expression of individual control over something, the right to informational self-determination, the right to privacy, and the right to data protection. In section 4.4., the focus is on data protection law, which is described as a two-fold regulation that has strong potential in recognising and granting individual control over data. In particular, the idea of individual control is enshrined in provisions on subjective rights and consent. Due to the limited scope of this work, the notion of consent is not discussed in detail, whereas control rights, representing the core issue of this thesis, are analysed more thoroughly. Finally, section 4.5. explains the reasons why, in the data-driven economy, control is a challenging aspiration. Three groups of factors – technological, psychological and economic – are identified as common challenges to data subject control.

4.2. Roots of the term

4.2.1. Ordinary language and dictionary meaning

In ordinary language, control has two dimensions. It implies that someone is, first, aware of a situation and, second, able to influence it. The second building block of control, i.e., the ability to influence, is central to the dictionary definition of the word. The Concise Oxford Dictionary defines control as the power to direct and to influence.⁵²⁰ Similarly, Merriam-Webster defines control as having power over or as exercising restraining or directing influence over someone or something.⁵²¹

Dictionary explanations of control are broad, open to different interpretations, and context-dependent. In the context of the data-driven economy, for instance, control requires influence over three stages in a data value chain: data collection, analytics, and data-driven decision-making.⁵²²

4.2.2. Control in philosophy

The concept of control corresponds to three pivotal philosophical notions: free will, liberty and autonomy. These three notions are seen as values, that is ideals or beliefs shared by a society about what is good and what is not, and function as normative anchors of fundamental human rights and principles. As mentioned above, these values are critical for individual well-being but can be undermined in the data-driven economy. The sections below briefly describe what role the notion of control plays in relation to them.

⁵²⁰ 'control', Oxford Living Online Dictionary <<https://en.oxforddictionaries.com/definition/control>> accessed 4 June 2018.

⁵²¹ 'control', Merriam-Webster Online Dictionary <<https://www.merriam-webster.com/dictionary/control>> accessed 4 June 2018.

⁵²² Compare Westin (2015) 5, who similarly distinguishes three control stages - control of when, how and to what extend information is communicated.

Free will ensures that a process or a situation is up to, or controlled by, the agent.⁵²³ Controlling the process requires true alternative possibilities. When this is the case, an agent also becomes morally responsible for what he does.⁵²⁴

A notion that is related to and sometimes overlaps with the concept of free will is that of individual liberty. In ordinary language, liberty refers to the quality or state of being free, and entails the power to do as one pleases, the freedom from physical restraint, the freedom from arbitrary or despotic control, and also the power of choice.⁵²⁵ In philosophical discussions, liberty is often split into two subcategories: negative and positive freedom. ‘Negative freedom’ refers to freedom from interference, to the absence of something, whereas ‘positive freedom’ refers to what we are free to do and is thus associated with the presence of something. This something is typically described as self-mastery, self-determination, self-realisation, and, finally, control. The concept of positive freedom is often used in relation to data protection as a manifestation of individual self-determination and control.⁵²⁶

In general, autonomy is attributed to a person when this person has *de facto power and authority* to direct affairs of elemental importance to her life within a framework of rules (or values, principles, beliefs, pro-attitudes) that she has set for herself.⁵²⁷ In other words, when agents have control, they should in principle have autonomy. However, agents can be deprived of their autonomy by brainwashing, depression, anxiety, or fatigue; and they can succumb to compulsions and addictions.⁵²⁸ Thus, exercising control does not always translate to having full autonomy. An example can be found in the medical field: consent to share medical data signed by a mentally ill person demonstrates some control, but due to the person’s special circumstances his control lacks true autonomy.⁵²⁹

In philosophical conceptualisations, control is closely related to some key values. If effective control is absent, values deteriorate too. In addition, effective control over data is linked with moral responsibility of data subjects for their actions regarding data. For instance, when control mechanisms such as consent do not translate to actual autonomy and free will, e.g. because of a data subject’s inability to understand the process or because no true alternatives exist, then this affects the level to which a data subject can be held responsible.

4.2.3. Control in psychology⁵³⁰

Typically, psychologists define control as the ability of an agent to intentionally produce desired outcomes and prevent undesired ones.⁵³¹ Skinner stresses that a sense of control is a robust predictor of physical and mental well-being. In her framework, control is strongly associated with autonomy,

⁵²³ Stanford Encyclopedia of Philosophy <<https://plato.stanford.edu/entries/freewill/>> accessed 4 June 2018.

⁵²⁴ Harry G Frankfurt, ‘Alternate Possibilities and Moral Responsibility’ (1969) 66 *The Journal of Philosophy* 829, 830.

⁵²⁵ Merriam-Webster Online Dictionary <<https://www.merriam-webster.com/dictionary/liberty>> accessed 4 June 2018.

⁵²⁶ See for example Jeanne Pia Mifsud Bonnici, ‘Exploring the Non-Absolute Nature of the Right to Data Protection’ (2014) 28 *International Review of Law, Computers & Technology* 131, 138.

⁵²⁷ Marina Oshana, ‘Autonomy and the Question of Authenticity’ (2007) 33 *Social Theory and Practice* 411.

⁵²⁸ Stanford Encyclopedia of Philosophy <<https://plato.stanford.edu/entries/personal-autonomy/>> accessed 4 June 2016.

⁵²⁹ Of course, the law mitigates this problem by requiring a valid consent which includes person conscience and understanding. See for example the Convention on Human Rights and Biomedicine (Oviedo Convention), Article 5 <<https://rm.coe.int/168007cf98>> accessed 15 August 2018.

⁵³⁰ This section uses excerpts from the article by Helena U Vrabec and Iris van Ooijen, ‘Does the GDPR Enhance Consumers’ Control over Personal Data?: An Analysis From a Behavioural Perspective’ (2018) *Journal of Consumer Policy*, 1-17.

⁵³¹ Ellen Skinner, ‘A Guide to Constructs of Control 71(3)’ (1996) 71 *Journal of Personality and Social Psychology* 549, 554.

self-determination, and perceived freedom.⁵³² Among the antecedents of control, Skinner lists information, choice, and predictability.⁵³³

A fundamental distinction in the literature on control is the one between actual and perceived control. This distinction is critical since experienced control (i.e., beliefs or experiences), rather than actual control, has psychological consequences.⁵³⁴ In other words, changes in actual control will only have psychological consequences if the person's beliefs or experiences change. For example, a person may formally have the ability to exert increased control on the storage and distribution of her personal data by search engines, but if the process to prevent storage and distribution of this data is perceived as incredibly complex, then control is not experienced as such. Therefore, increased actual control may not result in experiences of self-determination and autonomy. On the other hand, the illusion of control entails that perceived control in a given situation is high, while in fact actual control may be low. For instance, a consumer may perceive that he has control over the extent to which his personal information is collected and distributed by a social network site because this website offers to alter its privacy settings.⁵³⁵ However, by explicitly providing this possibility only for a part of the privacy settings, and leaving out other information (for instance, that the information will be distributed to third parties), the data collector creates a false sense of control and generates information asymmetry between itself and the individual. Although perceived control may increase in such a situation (along with experiences of self-determination and autonomy), actual control deteriorates.

The distinction between actual and perceived control is relevant to the discussion on control within law. When control is structurally not experienced as such, regulation will fail to empower consumers to control their personal data. Knowledge of the factors that stimulate perception of control may contribute to the development of policies that enhance consumer control and, consequently, their well-being. In principle, policies should encourage situations in which both perceived and actual control are present. However, Acquisti et al. write about a paradox that occurs with privacy enabling technologies (PETs).⁵³⁶ Whereas PETs in theory lead to enhanced control (actual and perceived), the feeling of security conveyed by the provision of fine-grained privacy controls lowers concerns and

⁵³² Ibid., 550.

⁵³³ Ibid., 555. This establishes an interesting parallel to data protection law. Consent provision, which is an important manifestation of individual control over data in data protection laws, requires that individual is informed about data processing, has the possibility to predict (to a reasonable degree) future data uses and is given a valid choice to either approve or disapprove data processing. Hence, psychological antecedents of control overlap with conditions for exercising control over personal data in the legal sense.

⁵³⁴ See for example Jerry M Burger, 'Negative Reactions to Increases in Perceived Personal Control' (1989) 56 *Journal of Personality and Social Psychology* 246.

⁵³⁵ In the aftermath of the data mining scandal in March 2018, Facebook decided to offer stronger privacy controls to individuals. *'In the coming months, privacy controls that are now in 20 places on Facebook's app will be merged into a single page, and will include what the company says will be easier-to-comprehend features that explain how the company is using a person's data, the company announced. [...] Facebook also will create a page that makes it easier for people to download their data so that they can more clearly view what information the company collects about them.'* Elizabeth Dwoskin and Tony Romm, 'Facebook makes its privacy controls simpler as company faces data reckoning' *The Washington Post* (28 March 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/03/28/facebooks-makes-its-privacy-controls-simpler-as-company-faces-data-reckoning/?utm_term=.f330e90d2ba9> accessed 3 June 2018.

⁵³⁶ Laura Brandimarte, Alessandro Acquisti and George Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox' (2012) 4 *Social Psychological and Personality Science* 4(3) 340.

drives those provided with such protections to reveal more sensitive information to a larger audience.⁵³⁷

Psychological studies show that within the increasingly complex data economy, privacy by control is more an inspiration than a realistic goal.⁵³⁸ The combination of bounded rationality, the tendency of consumers to attend to the online environment with only partial attention, and the increased (risk of) vulnerability and uncertainty that are associated with online data transactions cause consumers to surrender and disclose their personal data beyond what is desired.⁵³⁹ On these grounds, the very possibility of control by the conventional figure of 'rational and autonomous agent' is seriously questioned.⁵⁴⁰

4.3. Individual control over data and fundamental rights

In the philosophical and psychological discourse the notion of individual control is closely related to some important values, such as self-determination, freedom, autonomy, and privacy. These values are normative anchors for the fundamental rights and principles enshrined in the EU primary law.

Just like the notion of control is integrated in the values, it is also reflected in the principles and rights that these values underpin.⁵⁴¹ For example, in relation to the right to data protection, control has been enshrined in the provisions of several legal treaties and fundamental documents, such as in the German Constitution, the ECHR as interpreted by the ECtHR, and, arguably, the US Constitution.⁵⁴² For this thesis, it is of particular importance to determine if/how control is addressed on the EU level, in particular in the EU Charter. Below, three rights from the EU Charter are explained in light of the underlying idea of control: the right to informational self-determination, the right to privacy and data protection, and the right to property. The right to informational self-determination is not explicated in the Charter but influenced its drafting process as an important source of inspiration.⁵⁴³

4.3.1. Control over personal data and the right to informational self-determination

Self-determination as a right is a fundamental issue in contemporary international law. It denotes people's legal right to decide their own destiny in the international order. In other words, it means removing illegitimate (foreign sovereign) powers and bringing control over government back to the genuine nation.⁵⁴⁴ *Informational self-determination* embodies a similar idea of control, i.e. deciding

⁵³⁷ Ibid.

⁵³⁸ See for instance Bernadette Kamleitner and Vincent-Wayne Mitchell, 'Can Consumers Experience Ownership for Their Personal Data? From Issues of Scope and Invisibility to Agents Handling Our Digital Blueprints BT - Psychological Ownership and Consumer Behavior' in Joann Peck and Suzanne B Shu (eds) (Springer International Publishing 2018).

⁵³⁹ See also Christophe Lazaro and Daniel Le Métayer, 'The Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPT-ed 4, n 3, quoting A Acquisti and J Grossklags, 'What Can Behavioral Economics Teach Us About Privacy' in A Acquisti et al (eds), *Digital Privacy. Theory, Technologies, and Practices* (New York: Auerbach Publications, 2007).

⁵⁴⁰ Ibid.

⁵⁴¹ Principles are fundamental truths or doctrines of law; comprehensive rules or doctrines which furnish a basis or origin for others; settled rules of action, procedure, or legal determination <<https://thelawdictionary.org/principles/>> accessed 4 June 2018. Rights are privileges that if challenged are supported in court <<https://thelawdictionary.org/legal-right/>> accessed 4 June 2018.

⁵⁴² Gabriel Stilman, 'The Right to Our Personal Memories: Informational Self-Determination and the Right to Record and Disclose Our Personal Data' (2015) 25 Journal of Evolution and Technology 14, 15.

⁵⁴³ Hijmans (2016) 60.

⁵⁴⁴ Karen Parker, 'Understanding Self-Determination: The Basics' (presentation at the First International Conference on the Right to Self-Determination, Geneva 2000) <<http://www.guidetoaction.org/parker/selfdet.html>> accessed 4 June 2018.

over the destiny of individual data and directing data uses. More specifically, this right provides individuals with the power to decide for themselves about issues of collection, disclosure, and use of their personal data.⁵⁴⁵ The right to self-determination was first explicated in 1983 by the German Constitutional Court, which found its roots in the first article of German Basic Law (German Constitution) focused on protecting personality rights including human dignity.⁵⁴⁶ In the landmark decision, the Court drew on the notion of self-determination to tackle the issue of privacy and integrity of IT systems in relation to population census.⁵⁴⁷ The Court not only held that individuals should be protected against the unrestricted collection, storage, use, and transfer of their personal data, but also insisted that individuals were afforded the freedom to decide whether to engage in or desist from certain activities that involve the use of their data. The ability to exercise freedom to decide, which the court also referred to as ‘control’, can be easily compromised in the context of modern data processing: *‘The freedom of individuals to make plans or decisions in reliance on their personal powers of self-determination may be significantly inhibited if they cannot with sufficient certainty determine what information on them is known in certain areas of their social sphere and in some measure appraise the extent of knowledge in the possession of possible interlocutors.’* Thus, the idea of control that individuals should maintain over their data is the essential argument expressed by the Court (though the Court also clearly stressed that this control might be limited under the principle of proportionality).

The German Constitutional Court’s interpretation of the right to self-determination inspired the drafters of the EU Charter. In fact, some see informational self-determination as a main source for Article 8 on the right to data protection.⁵⁴⁸ This is not surprising, because informational self-determination and data protection have two corresponding effects. The first is preventing sensitive information from shifting from one context (e.g. the working world, medical treatment, family life, etc.) into other ones, thus creating a sphere in which an individual can feel safe and act free from any interference.⁵⁴⁹ This equals informational self-determination in the traditional sense, meaning the right to determine what personal data is disclosed, to whom, and for what purposes it is used.⁵⁵⁰ The second effect refers to the broader understanding of informational self-determination as the precondition for citizens’ un-biased participation in the political processes of the democratic constitutional state and on the markets.⁵⁵¹ The German Constitutional Court has drawn an explicit link to the threat to free democratic society if informational self-determination is not adequately protected.⁵⁵² Democratic deficit can also arise as a result of data controllers’ profit-oriented behaviour, which causes strong power asymmetries. As explained in Chapter 2, the world’s largest data holders have acquired great powers over data. They have even taken the government’s place by exercising a supervisory role over the data economy, where government command has often proved ineffective.⁵⁵³ These power

⁵⁴⁵ Stilman (2015) 15, quoting Westin and Kommers.

⁵⁴⁶ Bundesverfassungsgericht, Urteil vom 15.12.1983, BverfGE 65, 1, 41.

⁵⁴⁷ English translation of the judgement <<https://freiheitsfoo.de/census-act/>> accessed 4 June 2018.

⁵⁴⁸ Jan Philipp Albrecht, ‘Hands Off Our Data!’ <https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf> 25.

⁵⁴⁹ Hornung and Schnabel (2009) 86.

⁵⁵⁰ Simone Fischer-Hübner and others, ‘Online Privacy: Towards Informational Self-Determination on the Internet’ in Mireille Hildebrandt and others (eds), *Digital Enlightenment Yearbook 2013* (2013) 124.

⁵⁵¹ Hornung and Schnabel (2009) 86.

⁵⁵² See II.1.a of the judgement. For the English translation see <<https://freiheitsfoo.de/census-act/>> accessed 4 June 2018.

⁵⁵³ Klonick (2018).

asymmetries have led to undesirable consequences such as abuses of individual digital identities,⁵⁵⁴ filter bubbles,⁵⁵⁵ and fake news.⁵⁵⁶ Not only does this influence an individual, it also influences society as a whole. By constraining data controllers' behaviour to fit the legal boundaries, informational self-determination and data protection both protect vital collective goods.

4.3.2. Control over personal data and the right to privacy

As explained in Chapter 3, the EU Charter's Article 7 is a broad provision. It was first conceptualised as 'seclusion' (opacity, or privacy as solitude),⁵⁵⁷ before being understood as also encompassing a dimension of 'non-interference' (decisional privacy, or privacy as liberty)⁵⁵⁸ and, finally, of individual informational control or empowerment (the ability of an individual to control the terms under which his personal information is acquired and used).⁵⁵⁹ This last conceptualisation of the right to privacy has come to the fore in Alan Westin's modern definition of privacy as a claim (or a right) of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others,⁵⁶⁰ and has often been framed as 'privacy as control'.⁵⁶¹ Some US commentators understood privacy as control as a synonym for a bundle of legal rights of ownership, such as rights of possession, alienability, exclusion of others, commercial ex- exploitation, and so on.⁵⁶² From the US, the idea of privacy as control was brought to the EU⁵⁶³ but was never widely accepted. In the EU, the concept of individual control has been used in two ways: as a definitional aspect of privacy and as an instrumental mechanism to realise valuable outcomes such as autonomy and freedom.⁵⁶⁴ However, privacy as control has never been understood as a set of traditional ownership rights, but only as a set of specific rights that concern preserving individual respect and human dignity.⁵⁶⁵

The ECHR and the EU Charter do not mention control as a specific aspect of privacy, but European courts have already shown that their interpretation of privacy extends far enough to capture the notion of control over personal data. For example, before the EU Charter was adopted (pre-2009), the CJEU drew on some aspects of control over personal data in the decisions in the cases *Rundfunk*,⁵⁶⁶

⁵⁵⁴ On abuse of individual identity see Botsman Rachel, 'Big data meets Big Brother as China moves to rate its citizens' *Wired* (21 October 2018) <<http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>> accessed 4 June 2018.

⁵⁵⁵ On filter bubbles see Frederik J Zuiderveen Borgesius and others, 'Should We Worry about Filter Bubbles?' (2016) 5 *Internet Policy Review* 1.

⁵⁵⁶ On fake news see Robyn Caplan, Lauren Hanson and Joan Donovan, 'Moderation After "Fake News"' (2018) <https://datasociety.net/pubs/oh/DataAndSociety_Deaf_Reckoning_2018.pdf> accessed 4 June 2018.

⁵⁵⁷ This perspective implies that too much access to a person interferes with privacy. Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' 398. See also De Hert and Gutwirth (2006).

⁵⁵⁸ Coming close to what Borgesius calls '*freedom from unreasonable constraints on identity construction*'. Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' 126.

⁵⁵⁹ Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds) *Reinventing Data Protection?* (Springer Netherlands 2009) 62.

⁵⁶⁰ Westin (2015) 5.

⁵⁶¹ Solove (2004) 76.

⁵⁶² *Ibid.*, 77.

⁵⁶³ Nadezhda Purtova, 'Property Rights in Personal Data: Learning from the American Discourse' (2009) 25 *Computer Law & Security Review* 507.

⁵⁶⁴ Koops and others (2016) 38.

⁵⁶⁵ *Ibid.*

⁵⁶⁶ C-465/00, *Rundfunk* ECLI:EU:C:2003:294, 20 May 2003.

Satamedia,⁵⁶⁷ and *Bavarian Lager*.⁵⁶⁸ In *Rundfunk*, the Court considered that an employee's lack of control over flows of her personal data resulted in a violation of the right to privacy.⁵⁶⁹

4.3.3. Control over personal data and the right to data protection

One of the reasons that the German Constitutional Court created the right to informational self-determination by drawing on the personality rights was that there was no other provision in the German Constitution that could help the Court deal with fundamental tensions in relation to data protection. The EU legal order, however, incorporates two such provisions: the right to privacy and the right to personal data protection. The latter in particular is centred around the idea of control over personal data. In fact, the ability of an individual to control the terms under which his personal information is acquired and used is often presented as the hallmark of data protection.⁵⁷⁰ The right to personal data protection sets out rules on the mechanisms to process personal data and *empowers* one to take steps – i.e., it is a dynamic kind of protection, which follows data in all its movements.⁵⁷¹ It can be argued that this accentuated control which must be in place regardless of whether the data has been made public or not (i.e. the right to privacy does not apply) is what distinguishes data protection from other fundamental provisions and justifies its individual positioning in the EU Charter.⁵⁷² For these reasons, Lynskey attributes to control the role of a normative anchor for personal data protection as a fundamental right.⁵⁷³ The control aspect of the right seems to be the best-fitting response to tangible and, in particular, intangible harms, such as power asymmetries, powerlessness of data subjects, and even discrimination and manipulation caused by modern data processing. With fully transparent data processing and perfect individual control over behavioural targeting data, the risk of manipulation could be reduced.⁵⁷⁴ For example, if e-commerce businesses were required to clearly present information about price discrimination when it worked to a consumer's disadvantage, manipulation with the help of personal data processing could be avoided.⁵⁷⁵ In addition, the obligation of data controllers to render the rights of data subjects more effective would adjust the balance of power between data subjects and controllers.⁵⁷⁶

Before the analysis continues, one additional remark is necessary. Traditionally, fundamental rights are 'conceived as liberties', consisting of relatively simple, aspirational statements.⁵⁷⁷ Administration of these rights is delegated to contemporary human rights institutions.⁵⁷⁸ Fundamental rights that reflect control over data, in particular the right to data protection, differ from that 'right-conceived-as-liberty' approach and should instead be described as a 'right-conceived-as-affordance', i.e. a right granting individuals a possibility to act.⁵⁷⁹ Similar to private law entitlements, the strength of the 'right-

⁵⁶⁷ C-73/07, *Satakunnan Markkinapörssi and Satamedia* ECLI:EU:C:2008:727, 16 December 2008.

⁵⁶⁸ C- 28/08, *Bavarian Lager*, ECLI:EU:C:2010:378, 29 June 2010.

⁵⁶⁹ *Supra* n 566, para. 73.

⁵⁷⁰ Rouvroy and Poullet (2009) 68.

⁵⁷¹ Rodotà (2009) 79.

⁵⁷² Lynskey (2015) 192.

⁵⁷³ *Ibid.*

⁵⁷⁴ Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' 127.

⁵⁷⁵ Borgesius and Poort (2017).

⁵⁷⁶ Lynskey (2015) 214.

⁵⁷⁷ Julie E Cohen, 'Affording Fundamental Rights' (2017) 4 Critical Analysis of Law 3-4.

⁵⁷⁸ *Ibid.*

⁵⁷⁹ *Ibid.*

conceived-as-affordance' is that it empowers individual citizens; the disadvantage is that this right also needs to be invoked by individuals.⁵⁸⁰

4.3.4. Control over personal data and the right to property

Protocol 1 to the ECHR defines property as the 'right to peaceful enjoyment of possessions'.⁵⁸¹ The state is only allowed to take control over personal property under strict conditions. *A contrario*, save for those exceptional situations, the right to property symbolises control exercised by an individual person.

As explained above, property is a general term for rules governing access to and *control* of land and other material resources.⁵⁸² All property law regimes have one common idea: the ability to exercise control over a thing. This type of control is characterised by its *erga omnes* effect, meaning that control spreads not only to persons or entities with whom someone contracts (e.g. not only to a buyer of a car), but to everyone in the world (e.g. to a potential thief of the car). However, the actual rigour of control depends on the type of property and/or ownership.⁵⁸³

With property rights regarding physical goods, the owner typically has exclusive rights and control over a good; in contrast, this is not the case for intangibles such as data.⁵⁸⁴ Property in data challenges traditional concepts of civil law, which since Roman times have attributed property to tangible goods. Roman concepts of *ius utendi*, *fructu et abutendi* are the most prominent examples of proprietary entitlements, and frankly, one can hardly imagine them being vested in bits of data.⁵⁸⁵ Because of these shortcomings, intellectual property rights are typically suggested as the legal means to establish clear ownership and, consequently, control. For structured databases, a *sui generis* database right was created by the EU database protection directive, which protects the 'substantial investment in either the obtaining, verification or presentation of the contents'.⁵⁸⁶

In principle, personal data is no different than any other data, as it is equally intangible and thus the same argument against vesting property rights in data would apply. However, in the data-driven economy data is viewed as a valuable asset, the new oil, and, consequently, a rivalrous good. For example, new business models on the Internet and social media use the so-called *freemium* pricing strategies, in which users obtain services for free but 'pay' with their personal data, often without their own knowledge.⁵⁸⁷ While consumers are not charged for the product, they themselves become a

⁵⁸⁰ Eric Tjong Tjin Tai, 'The Right to Be Forgotten - Private Law Enforcement' (2017) 8 <<https://ssrn.com/abstract=2958145>> accessed 4 June 2018.

⁵⁸¹ Protocol 1 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Article 1.

⁵⁸² Stanford Encyclopedia of Philosophy <<https://plato.stanford.edu/entries/property/>> accessed 4 June 2018.

⁵⁸³ For instance, lease is a weaker property right than ownership of a land. However, a 999-year lease may come very close to ownership. Elizabeth Cooke, *Land Law* (Oxford University Press 2012) 4.

⁵⁸⁴ Data are an intangible asset, which in many ways match the public good character of information and knowledge, at least with respect to non-rivalry in use. Ingrid Schneider, 'Big Data, IP, Data Ownership and Privacy: Conceptualising a Conundrum' (Presentation at the 10th Annual Conference of the EPIP Association in Glasgow, 2015) <<http://www.epip2015.org/big-data-ip-data-ownership-and-privacy-conceptualising-a-conundrum/>> accessed 4 June 2016. Like other information-related goods, they can be reproduced and transferred at almost zero marginal costs. OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' 195.

⁵⁸⁵ William Edward Hearn, *Theory of legal duties and rights* (1883) 186.

⁵⁸⁶ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 77/20 [1996] 27 March 1996, Article 7(1).

⁵⁸⁷ European Commission Staff, 'Online Platforms - Accompanying the Document Communication Communication on Online Platforms and the Digital Single Market' (2016) 33.

product by sharing their data.⁵⁸⁸ Furthermore, some recent competition law cases concerning market power related to the availability of users' data are another indication of data commodification occurring in the real world.⁵⁸⁹ This explains the relevance of the property discourse on personal data.

If personal data was regulated as property, it would fall under the complete control of individuals, producing *erga omnes* effects. Some have suggested that propertisation of personal data would be a good fit for the current economic situation.⁵⁹⁰ Property would give personal data protection an *erga omnes* effect – the legal owner of data would be entitled to control that data regardless of its current location (e.g. somewhere on the premises of a third party). In this way, propertisation would be a response to users' decreasing control in the data economy, which is becoming increasingly difficult to exercise.⁵⁹¹

However, EU data protection law is at odds with the idea of ultimate control suggested by the advocates of propertisation. The right to data protection is focused on one's personality, not one's property.⁵⁹² While it is true that both rights, the right to property and the right to data protection, entail some control, the nature of control vested in the two rights differs. The control in property law is ultimate, i.e. entails the ability to give up the object of property and leave the decisions about it up to a third party. In contrast, the control in data protection law does not extend that far, i.e. some entitlements can never be alienable. This seems to be the right balance. Findings from psychological research suggest that a person, because of her bounded rationality, often inappropriately reacts to data processing threats (or does not react at all). Therefore, some degree of legislative paternalism in the sense of limited control is indispensable. In addition, the view of data protection as a human right takes into account the rights of other actors in society. These are recognized in Article 6 of the GDPR which introduces various legal bases for data processing such as public interest and research objectives.

For the above reasons, it would be difficult to claim that the EU law has adopted or could adopt a property regime. The EU legal system clearly prefers the view of control enabled by the human rights (including the data protection right) paradigm over the view of control enabled by the property paradigm. That being said, the EU data protection legislation does incorporate a few property-like entitlements.⁵⁹³ For instance, some property features can be seen in the newly established right to data portability, which allows the data subject not only to obtain a copy for his own use, but also 'to transmit those personal data [...] into another [processing system], in an electronic format which is commonly used' when the data subject has provided these data.⁵⁹⁴

4.4. Control and EU data protection law

Contrary to the normative conceptualisations of control explored in section 4.3. on fundamental rights, the notion of control becomes more tangible on the level of secondary law, coming closer to what

⁵⁸⁸ Tene and Polonetsky (2013) 255.

⁵⁸⁹ See section 3.3.4.

⁵⁹⁰ Lessig (2006) 228-231.

⁵⁹¹ Ibid.

⁵⁹² Rodotà (2009) 81.

⁵⁹³ Nadezha Purtova, 'Property in Personal Data' (Tilburg University 2011); Jakob M Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 *The Yale Law Journal* 513.

⁵⁹⁴ Purtova (2011) 25.

Black's Law Dictionary describes as a power to direct, manage, oversee, and/or restrict the affairs, business, or assets of a person or entity.⁵⁹⁵ Control features can be found in several legal domains: in property law through ownership entitlements, corporate law through the division of roles between owners and managers, consumer protection law through the right to information and withdrawal, and data protection law through (among others) data subject control rights. The latter is of particular interest for this study.

4.4.1. Policy vision for individual control in the data-driven economy

EU policy documents preceding the new EU regulation on personal data suggested that the concept of data subject control most genuinely reflects the contemporary understanding of personal data protection.⁵⁹⁶ In 2011, when explaining the blueprint for the future EU regulation on data protection, Vivian Reding pointed to individual control as a central notion in the legal reform: *'I am a firm believer in the necessity of enhancing individuals' control over their own data.'* In her speech, Reding envisioned four pillars of individual control that should form the basis of the upcoming legislation: the right to be forgotten, transparency (information), privacy by default (consent), and protection regardless of data location.⁵⁹⁷

During the legislative process, Reding's ideas were somewhat watered down. For example, after the intense lobbying from some leading business representatives, the right to be forgotten lost its initial strength. Nevertheless, control was preserved in the GDPR's final version as an important underlying idea: *'Natural persons should have control of their own personal data,'* reads Recital 7. Moreover, Reding's pillars idea found its way in the enhanced section on control rights and the updated provision on consent.

During the GDPR adoption process, the notion of control emerged several times in legislative and policy documents of highly diverse natures, ranging from preparatory works for legislation and legislative text, to experts' opinions and vulgarised material addressed to citizens, e.g., in the 2012 Communication from the Commission 'Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century'; in the 2012 European Commission brochure and movie 'Take control of your personal data'; and in the 2010 Communication 'A comprehensive approach on personal data protection in the European Union'.⁵⁹⁸ In particular, data subject rights were put forward as a tool at the disposal of the data subjects to enable them to be in control at the different stages of the processing of their data.^{599,600}

⁵⁹⁵ 'control' *Black's Law Dictionary* (1910).

⁵⁹⁶ In particular those pertaining to the Regulation, such as the Commission's proposal. *Supra* n 30. Also see European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union' (2010).

⁵⁹⁷ Viviane Reding, 'SPEECH 11/183 Your data, your rights: Safeguarding your privacy in a connected world' (Brussels, 16 March 2011) <http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm> accessed 4 June 2018.

⁵⁹⁸ Lazaro and Métayer (2015) 17-18.

⁵⁹⁹ Lynskey (2015).

⁶⁰⁰ The European Commission was vocal in conveying the idea of control over (personal and non-personal) data in relation to the growing European data economy. In its plans on future regulation of data flows, the Commission discussed how assigning control to a particular entity would contribute to a boost of the data economy. For example, the Commission discussed control in the context of data traceability: *'Traceability and clear identification of data sources are a precondition for real control of data in the market.'* European Commission, 'Communication from the Commission to the EU Parliament,

The Article 29 Working Party discussed control in some of its influential publications. For example, in the opinion on consent from 2011, it held that *'[i]f it is correctly used, consent is a tool giving the data subject control over the processing of his data.'* In the guidelines on the right to data portability, it stressed that *'[t]he purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.'*⁶⁰¹

The diversity of authorities and documents that have dealt with the concept illustrates the pervasiveness of the rhetoric of control on the EU level.⁶⁰² However, this rhetoric was not adopted by the Court of Justice. A brief review of the recent case law indicates no particular intention of the Court to follow the control-oriented policy diction, though this cannot be excluded in the future. It should be kept in mind that some of the CJEU's judgements could be interpreted as arguing for informational control.⁶⁰³ In addition, the Advocate Generals' opinions, which often pave the way for the CJEU judgements, often draw on the Article 29 Working Party's opinions. Therefore, it is plausible that its views on control could be influential in, for instance, future decisions on data portability.⁶⁰⁴

4.4.2. Reflections of control in the GDPR

As explained in the previous chapter, the GDPR is the EU's key legal act regulating the processing of personal data in the data-driven economy. Control over personal data is reflected in several data protection legal mechanisms, most apparently in the provisions on consent and control rights. Clearly, control is not an exclusive objective of EU data protection law. On the contrary, rules in data protection law are two-fold: they either relate to control over personal data or to protection of personal data. The first group is directed to individuals and enhances their control over data, whereas the second is directed to data holders and imposes a duty on them to protect personal data. In the data-driven economy, actual control over data most often lies in the hands of (big) data controllers. The aim of the law is to limit this control by imposing protection duties and tilting the balance in favour of *individual* control that stems from personal autonomy and other values.

The EU data protection law is thus an inherently binary legislation. However, the control side has recently garnered more attention. The GDPR has strengthened and extended provisions on data subject control and consent. Policy documents and opinions explained above restate the same vision. Interestingly, this policy vision is in strong contrast with the current situation in the data economy. As shown in Chapters 1 and 2, the information outburst has led to a situation in which consumers are inevitably losing control over their data. The divergence between the harsh economic reality and the regulatory utopia makes control-related provisions both highly relevant and potentially controversial.

the Council the European Economic and Social Committee and the Committee of the Regions - Building a European Data Economy' (2017) 12.

⁶⁰¹ The Working Party also addressed control in the opinion on the concepts of controller and processor from 2010. However, this is a different type of control than the one discussed in relation to individuals. Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (2010).

⁶⁰² Lazaro and Métayer (2015) 15.

⁶⁰³ Most apparently, in the Google Spain case (*Google Spain*, C-131/12, ECLI:EU:C:2014:317). Also see the judgement of 7 May 2009, *Rijkeboer* C-553/07, ECLI:EU:C:2009:293, para. 49.

⁶⁰⁴ See for example AG Opinion from 24 October 2017 in *Wirtschaftsakademie Schleswig-Holstein* C-210/16, ECLI:EU:C:2018:57, AG opinion from 12 May 2016 in *Breyer* C-582/14, ECLI:EU:C:2016:339, AG opinion from 25 June 2015 in *Weltimmo*, ECLI:EU:C:2015:426, AG opinion from 7 October 2014 in *Ryneš*, C-230/14, ECLI:EU:C:2014:2072, AG Opinion from 25 June 2013 in *Google Spain and Google*, C-131/12, ECLI:EU:C:2013:424.

Data protection control-related provisions can be split into two large groups: consent and data control rights.⁶⁰⁵ This indicates that individual control should extend to two stages in the data value chain: data collection and secondary uses of data.⁶⁰⁶ In the collection stage, consent and the right to information are the key principles. In the second stage, control rights such as the rights to be forgotten, to object, and to access are of particular importance.⁶⁰⁷

Consent pertains to the initial ‘yes’ or ‘no’ before data collection starts. However, the role of consent in controlling personal data collection is reduced for two reasons. First, consent does not give control over processing in all cases. If contract, legitimate interest, or public interest are used as a basis for data processing, the reach of consent is curtailed. Second, there is growing scepticism regarding the effectiveness of informed consent in the context of personal data processing, in particular in relation to the requirement for informed consent.⁶⁰⁸ Due to the complexity of data processing, being effectively informed has become nearly impossible. Overload of consent-seeking privacy notices has resulted in consent desensitisation.⁶⁰⁹ Users no longer make active, informed choices when confronted with a consent situation, but instead simply provide consent when asked to do so.⁶¹⁰

The GDPR explicitly allows for withdrawal of consent (Article 7(3)), but the option to withdraw faces as many challenges as consent itself.⁶¹¹ This makes the possibility of extending individual control through data subject consent beyond the data collection stage, i.e. into the secondary use stage, highly theoretical.

Control rights, on the other hand, offer more leeway. These rights apply when processing is based on consent or some other legal basis. This is important in addressing controversial secondary uses of data, which are often based on a contract or legitimate interest. Thus, data subject rights could to some extent work as use regulation (for instance, Article 22’s provision on automated decision-making) and thus enable control that extends beyond consent’s take-it-or-leave-it approach.⁶¹² Furthermore, having been strengthened by the CJEU’s recent interpretation and extended in the updated data protection law, data subject rights seem to somewhat adapt to the new data-driven reality.⁶¹³ To summarise, control rights seem to represent a key legal instrument to enhance individual control in the data-driven era. This justifies a detailed analysis of control rights in the following chapters.

4.4.3. Clustering control rights in the GDPR

The EU data protection reform in 2016 introduced an extended section on data subject rights. Under the GDPR regime, the catalogue of control rights consists of the following eight entitlements: the right to information (Articles 14 and 15), the right to access (Article 15), the right to rectification (Article 16),

⁶⁰⁵ See for example Lynskey (2015); Mantelero (2014); Lazaro and Métayer (2015).

⁶⁰⁶ Chapter 2 discussed stages of the data value chain in more detail.

⁶⁰⁷ In particular when processing is not based on consent.

⁶⁰⁸ Bart Custers, ‘Click Here to Consent Forever: Expiry Dates for Informed Consent’ (2016) 3 *Big Data & Society* 2.

⁶⁰⁹ Schermer, Custers and van der Hof (2013) 12.

⁶¹⁰ *Ibid.*

⁶¹¹ It creates a take-it-or-leave-it situation, assumes that nothing changes during the length of the contract and most users do not seem to cancel their free accounts anyway. Custers (2016) 4.

⁶¹² Joris Van Hoboken, ‘From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and Us Frameworks for Personal Data Processing’ in Bart Van Der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 237.

⁶¹³ See for example Brkan (2016).

the right to erasure/to be forgotten (Article 17), the right to restriction of processing (Article 18), the right to data portability (Article 20), the right to object, and the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning an individual or similarly significantly affects her (Articles 21 and 22).

One of the major amendments that the GDPR has brought to the existing data privacy laws is the enhancement of the package of rights of the data subject, strengthening and detailing existing ones, and introducing new ones.⁶¹⁴ This is in line with what was discussed in the previous section about the growing interest of regulators in increasing '*data subject control and empowerment*'. Indeed, the data-driven reality has opened the way to powerful data barons who seem to control our data more intensively (and more subtly) than ever before. Shifting some control towards consumers is a logical reaction.

In comparison to the DPD, the setup of data subject rights in the GDPR is significantly amended. While the directive listed the rights under Article 12 and, somewhat confusingly, grouped them as rights to access, the regulation has taken a much more structured approach. Chapter 2 of the GDPR splits the rights into different groups starting with transparency requirement and the right to information, going on to the rights to access, to erase, and to data portability. Interestingly, the right to information has clearly been made a part of the data subject rights bundle. Moreover, quite significantly, the GDPR now explicitly includes two new rights: the aforementioned right to erase (the right to be forgotten) and the right to data portability.

Drawing on EU statutory and case law, the following chapters provide a detailed analysis of data subject control rights. For the purpose of this analysis, the scope is limited to six rights:

1. The right to information, including the provisions on transparency,
2. The right to access,
3. The right to erasure,
4. The right to data portability,
5. The right to object, and the right not to be subjected to automated individual decision-making.⁶¹⁵

Each of the following chapters of this thesis (Chapters 5 to 9) refers to one of the points listed above. The selection appears in line with some earlier academic endeavours to organise the rights.⁶¹⁶ As a careful reader may note, some data subject rights (the right to rectification and the right to restriction) are disregarded. As mentioned in Chapter 1, this is not to say that these rights are irrelevant in the light of the big data discussion. The reason for the exclusion is that they share similarities with the right to

⁶¹⁴ Gabriela Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform' (2012) 6 International Data Privacy Law; Daniel Solove, '10 Implications of the New EU General Data Protection Regulation (GDPR)' *Teachprivacy* (23 December 2015) <<https://www.teachprivacy.com/new-eu-data-protection-regulation-gdpr/>> accessed 4 June 2018.

⁶¹⁵ An alternative way to organise the rights could be a two-fold division into the following two groups: 1. Information and access rights 2. Active rights incl. consent. Lazaro and Métayer (2015) 22-23. See also Dara Hallinan and others, 'PRESCIENT Deliverable 3: Privacy, Data Protection and Ethical Issues in New and Emerging Technologies; Assessing Citizens' Concerns and Knowledge of Stored Personal Data' (2012).

⁶¹⁶ See for instance Gabriela Zanfir, 'Drepturile Persoanei Vizate În Contextul Prelucrării Datelor Private' (University of Craiova 2013).

erasure (Article 17) and the right to object (Article 21). Thus, their limitations and prospects are, to a large extent, reflected in the analysis of the rights in Articles 17 and 21.⁶¹⁷

4.5. Individual control – a challenging aspiration

The previous section established that individual control represents a central notion in the system of EU data protection law. However, in the data-driven economy, individual control has become a challenging aspiration. Based on the findings in Chapter 2 and in section 4.2., it is possible to identify three types of technological, economic, and psychological causes, all of which are rooted in the specific characteristics of the data-driven economy, that weaken individual control. *Technological* causes refer to the intangible and invisible nature of data-driven technologies, which open up possibilities to duplicate and share data in opaque and less controlled ways than physical goods. In such an environment, it becomes much more difficult to exercise effective control over data. *Economic* causes refer to the market forces that have created a situation in which data barons' dominance over digital information is no longer counter-balanced by control of other actors. Data barons are companies that have access to a large amount of personal data, which makes them increasingly powerful. Data platforms, operating on a two-sided market, are a typical example.⁶¹⁸ To enrich data that is provided or generated by users, platforms acquire additional personal data by collaborating with data brokers or using open source data. Later, they recoup their investments by reusing the data or by sharing it with multiple parties.⁶¹⁹ This sort of data reuse is problematic because it is opaque, technologically complex,⁶²⁰ and therefore fundamentally challenges the idea of individual control. Finally, *psychological* causes often prevent individuals from exercising effective control over data. Data subjects lack the ability and motivation to scrutinise key details of personal data processing necessary to make informed decisions about their data.⁶²¹ The phenomenon of 'bounded rationality' adds to the problem. Individuals' judgements and decisions are often not reached on the basis of a rational optimisation process, but are instead the result of heuristic and biased information processing.⁶²²

4.6. Conclusions

By exploring the concept of control, this chapter answered the third research sub-question regarding the notion of individual control and its relation with data subject rights. While doing so, it established a bridge between the general overview of the data-driven economy and the pertaining legal framework, and the specific analysis of data subject control rights.

⁶¹⁷ That said, the rights may evolve into a more significant provision in the future. This will depend on the further guidance regarding the articles' scope of application. See Frederike Kaltheuner and Elettra Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2017) 2 Journal of Information Rights, Policy and Practice.

⁶¹⁸ Chapter 2, section 2.3.1.

⁶¹⁹ Will Oremus, 'The Real Scandal Isn't What Cambridge Analytica Did' *Slate.com* (March 20, 2018) <<https://slate.com/technology/2018/03/the-real-scandal-isnt-cambridge-analytica-its-facebooks-whole-business-model.html>> accessed 22 May 2018.

⁶²⁰ They also exceed regulatory expectations and supervisory powers. Pasquale (2015) 2.

⁶²¹ Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' [2016] TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy 2016, 19.

⁶²² Gigerenzer and Reinhard Selten, *Bounded Rationality: The Adaptive Toolbox* (MIT Press 2002).

Individual control represents a central notion in philosophical discussions related to people's autonomy and freedom. Lack of effective control translates into deterioration of some essential values. In psychology, control represents an essential condition for individual well-being.

Individual control over data plays a role in the provisions of primary and secondary EU law. On the primary law level, control is integrated in several fundamental rights. In the context of this study, the right to data protection stands out as its 'control' aspect links directly to data subject rights.

Among the secondary law sources, the notion of control stands out in data protection law. The analysis of the provisions in the latter reveals two facets of control: the first is normative, meaning that control links back to the values that underpin the entire legal field, while the second is instrumental and materialises through the provisions on data subject rights. This second facet is what the remaining chapters focus on.

In spite of being a central notion in data protection law, the notion of individual control undoubtedly faces many challenges. In particular, technological, economic, and psychological causes, all of which are rooted in the specific characteristics of the data-driven economy, weaken individual control. The remaining chapters will analyse to what extent data subject rights are resistant to these challenges or, in other words, how effectively these rights afford control to data subjects.