Book Reviews

The Book Reviews section will introduce you to the latest and most interesting books on a wide range of topics pertaining to the law and policy of data protection. For further information on the submission of reviews please contact the Book Reviews Editor Gloria González Fuster at Gloria.Gonzalez.Fuster@vub.be.

Privacy online, Law and the Effective Regulation of Online Services

by Marcin Betkier

Intersentia 2019; 286 pp.

€79.00; Hardback

Chiara Angiolini*

In his new book, *Privacy online, Law and the Effective Regulation of Online Services*, Marcin Betkier imagines and formulates a Privacy Management Model (PMM). The model aims to grant online informational self-determination to data subjects, taking into account the key-role of the use and sharing of personal data in the contemporary economy. In order to identify the issues showing the needs of such a model, and in order to build it, an interdisciplinary approach with a comparative legal perspective as the backbone is adopted.

The book is divided into two parts. The first one is devoted to an analysis of the justifications for the creation of a PMM and investigates the relationship between online service providers as data controllers and users of those services as data subjects. In the second part, the author develops and shapes the model.

In particular, the first part analyses the notion of personal data and its uses, with a focus on the roles of data controllers and data subjects in the online environment. It provides valuable taxonomies, which concern the groups of data controllers, the interests they pursue, the risk of processing for the data subject and the means which enable processing operations. The book then focuses on the relationship between data subjects and a specific category of data controllers, that is, online service providers which pursue commercial interests. In this respect, Betkier develops a categorisation of service provider business models that treat data as 'strategic assets'¹ that service providers aim to collect and use (eg for marketing purposes). Activities creating a risk of a lack

of control by the data subject are identified in all business models.

On the data subject side, the author deals with multiple dimensions and theories on data privacy. Relying on the concept of informational self-determination, privacy is defined as the 'ability to make one's own decisions as regards the disclosure and (separately) use of one's personal data',² maintaining a certain degree of control over data and their availability. The author highlights how the decision-making of data subjects regarding their privacy changes in relation to context and social roles and how there is a need to attribute greater importance and priority to data subject choices against standardized privacy policies drafted by online service providers.³ Different levels of influence that the data controller may exercise over the data subject are also analyzed.

Betskier furthermore identifies three 'privacy problems' generated by the actions of service providers and the characteristics of the online environment: the first is a risk of tangible (often economic) loss, the second an impediment to dignity and autonomy, and the third a detriment to social values. Regarding the first risk, the author looks at possible discrimination based on data processing and at eventual data subject manipulation, for example in targeting for marketing purposes, or in political elections (eg the case of Cambridge Analytica), as well as 'identity theft'. Betkier also considers how the consequences of mass-scale data collection and processing lead to a form of surveillance, which may endanger the ca-

DOI: 10.21552/edpl/2020/3/18

* Post-doctoral Researcher, Faculty of Law, Trento University. For correspondence: <chiara.angiolini@unitn.it>

1 Marcin Betkier, *Privacy online, Law and the Effective Regulation of Online Services*, (Intersentia 2019) 45.

2 *ibid*, 21.

3 *ibid*, 83.

capacity of autonomous action.⁴ In terms of the detriment to social values, the author highlights the negative consequences of the mass-scale collection and processing of personal data, with regard to freedom of expression and social manipulation, which is particularly relevant in political elections.

The analysis then focuses on consent as the key instrument that several jurisdictions have adopted in order to shape the relationship between data controllers and data subjects, with the aim of enabling the latter to make autonomous choices. The author sums up all the arguments which have led scholars to critically discuss the role of consent in ensuring a data subject's control over data and their empowerment: consent is often not (well) informed; in multiple cases there are no other meaningful choices for customers other than to give their consent; and making a rational choice when it comes to evaluating privacy risks and the economic benefits of online services is a complex endeavor. Furthermore, Betkier highlights how the relationship between service providers and users is mediated by technology, and that there is no personal communication between them. His conclusion is that consent is not an effective means of exercising personal autonomy in processes which consist of the collection, use and sharing of personal data.⁵ Therefore, tools that enable the data subject to control and *manage* data processing procedures are necessary. Studies on the price of personal data are also mentioned; they demonstrate how people have declared they would sell their own data for a price higher than that currently offered by service providers. Betkier thus concludes that personal data are in fact tradeable, and that these studies suggest how the actual agreements being made are not on an equal footing.

In accordance with the interdisciplinary methodology of the book, is provided an analysis of the technology which contributes to shaping the relationship between service providers and data subjects. The au-

thor stresses how the design of websites and apps narrows the possible actions of the user and to a certain extent predetermines them. In Betkier's view, the technological architecture of online services creates an information asymmetry between the user and the service provider. Based on his analysis from the first part of the book, the author states: 'there need to be countermeasures focusing on architectural and informational imbalances'.⁶

Accordingly, the second part of the book is devoted to formulating a Privacy Management Model, conceived of as a set of regulatory tools⁷ aimed at ensuring the effective management of personal data by data subjects, as well as enabling them to exercise their personal autonomy alongside the functioning of online markets based on the processing of personal data. Betkier considers both data subjects' informational self-determination and their role as a contractual party of an agreement concerning personal data. He affirms that data are traded on 'data markets'⁸ and that they provide a competitive advantage to those who use them. From a market-oriented perspective, the PMM aims at restoring equilibrium between parties, balancing out information asymmetries and fostering trust, as well as promoting competitiveness between service providers by enhancing data portability and reducing the 'lock-in mechanism'.⁹

In the author's view, the PMM performs three main functions: controlling, planning, and organizing. These activities are exercised by data subjects in an indirect way, because it is typically service providers that maintain a factual control over data. With regard to planning, the privacy policy chosen by the individual should have precedence over the default settings of service providers. Moreover, a data subject's choices should prevail over the default privacy settings drawn up by service providers.

Within the deep analysis made by the author, it is taken for granted that the relationship between the data subject and the data controller is contractual, and, due to the power imbalance between parties, a limitation of the freedom of contract is considered necessary. Within the PMM, the data subject should always exercise control over her data, through the PMM interface, by deleting it and/or changing privacy settings. Therefore, the PMM does not allow the data subject to sell personal data 'without the possibility of taking them back'¹⁰ and the online contract should foresee a change in privacy settings. Considering the academic and judicial debate on the applic-

4 *ibid.* The author states that 'controlling what individuals read or search for on the web means essentially controlling what they are thinking', 74.

5 *ibid.*, 36.

6 *ibid.*, 76.

7 *ibid.*, 80.

8 *ibid.*, 109.

9 *ibid.*, 98.

10 *ibid.*, 114.

ability of contract law to privacy policies, a deeper analysis of this issue would have been appropriate, with an eye towards the economic exploitation of data protection rights or data tradability. Such a study would have been particularly useful for investigating possible different applications of the concept of ‘individual autonomy’; a question arises as to whether its meaning and the related means of protection are different when it is applied as the underpinnings of the freedom of contract or as the core of informational self-determination, conceived as fundamental to the exercise of freedom and dignity in societal relationships, especially those of a political nature.

The organizing function is to be implemented by adopting the standardized and comprehensive categorization of data and data uses, which should be the same for all service providers. Such categorization aims at increasing the level of transparency and data awareness.¹¹ Furthermore, Betkier foresees the creation of user interfaces, which would permit data subjects to manage their own privacy settings.

The controlling function, finally, concerns the possibility for a data subject to view and change the parameters of the privacy process itself. For the author, the difference between the controlling function and consent is that, within the PMM, authorization is given by the data subject to standardized types of data and their particular uses, giving the data subject the ability to change her choices. The right to delete, access and export data are conceived as part of this function.

To summarize, the proposed privacy management model ideally allows the data subject to set and change the goals of processing, to implement individual policies and their execution, and to monitor and evaluate the results,¹² thereby enhancing informational autonomy. Data subjects should be able to manage personal data that concerns them from outside the environments established by service providers, and even import their preferred privacy settings within the service provider’s environment.

Throughout this process, individuals are not left on their own: the model is based on the existence of ‘trusted third parties’ called Personal Information Administrators (PIAs). The PIAs should ‘act on behalf of data subjects to manage personal data in the system of service providers’¹³ and give them advice. Given the role of PIAs, some additional rules are foreseen in order to prevent possible conflicts of interest;¹⁴ their power should be limited and subject to

control. Accordingly, PIAs should not be able to benefit directly from data¹⁵ and will only be involved in the flow of personal data as necessary to exercise a privacy management function¹⁶ and should not receive any benefits either directly or indirectly from service providers. Against this backdrop, the Data Protection Authorities would have a supervisory role.

Technology is an important aspect in the implementation of the PMM. A set of interfaces that could be used for adjusting privacy settings are foreseen. For example, Application Programming Interfaces (API) would enable PIAs ‘to build a software tool that integrates the management of data in the ICT systems of multiple service providers’ and through which the privacy choices of data subjects are transformed into controlling decisions concerning data. Chapter 6 is entirely devoted to the study of the technological tools necessary for implementing PMM and to make it effective.

The possibility of implementing the PMM model within existing legal frameworks is also the subject of analysis: Australian, Canadian, New Zealand and European laws are all taken into account and considered. Furthermore, the Fair Information Practice Principles (FIPPs), as enacted in several international acts and documents are considered. Betkier highlights how FIPPs are based on procedural rules which regulate the uses of personal data and which pursue the objective of balancing different interests (eg through the principles of purpose limitation). In his view, these principles would not enable the implementation of the privacy management model because the role of the data subject is not emphasized. Moreover, a meaningful classification of different regulatory approaches is provided, based on the possibility of a data subject’s autonomous choices and participation in the data processing operations they permit. The presence of elements of control, planning and organization are all considered within this analysis. As a result of this comparative study, Betkier concludes that national privacy laws make the implementation of the PMM possible to a certain ex-

11 *ibid*, 166-17.

12 *ibid*, 90.

13 *ibid*, 136.

14 *ibid*, 136.

15 *ibid*, 136.

16 *ibid*, 137.

tent, but they do not provide for such a model, because of a lack of planning and organizing aspects. The GDPR is seen as the most adequate legal environment for developing the privacy management model, considering that it fosters, at least to a certain extent, a data subject's participatory role in processing operations. Therefore, an analysis of changes to the GDPR that the implementation of the PMM would require is provided with regard to its control, planning and organizing function.

Furthermore, the introduction of some general rules is foreseen. Firstly, the author calls for the adoption of the substantive right to informational self-determination, which would consist of the right to determine for oneself whether personal data may be collected or disclosed and how they may be used. This right is seen as necessary for effective regulation, because it provides data subjects with a strong entitlement and it defines quite clearly the data subjects' interest in data that concerns them. The second general rule deals with the field of application of data protection laws; Betkier calls for mechanisms that would ensure a certain degree of extraterritorial application of the law.

Moreover, the author proposes the introduction of a *lex specialis* to data privacy laws, applicable to data controllers which might 'potentially breach informational autonomy,' ie the ones who 'use personal data outside the context of the particular transaction recognizable by the data subject'¹⁷ (eg entities offering online advertising or that profile data subjects).

Overall, the book is a valuable and remarkable read for at least two reasons. First, it provides a meaningful description of the relationship that exists between online service providers as data controllers and users as data subjects, as well as an insightful overview of existing problematic issues and a discussion of legislative frameworks. Second, Betkier proposes a new model which would shape this relationship based on two strong ideas: the 'individual privacy policy' that should prevail over privacy policies drafted by service providers and the well-defined role of Personal Information Administrators (PIAs).

Privacy Online, Law and the Effective Regulation of Online Services should be of great interest to different readers. Data protection researchers can find a critical analysis of existing data protection issues related to online services as well as an original proposal for solving them. Regulators and data protection experts might be interested in the Privacy Management Model, which could give them precious insights towards the possible modification of the existing legal framework and ICT technological architecture.

The Right to Erasure in EU Data Protection Law

by Jef Ausloos

Oxford University Press 2020; 560 pp.

£70.00; Hardback

*Axel Freiherr von dem Bussche**

Jef Ausloos' book 'The Right to Erasure in EU Data Protection Law', published in 2020 by Oxford University Press, is not a typical legal textbook, as it is based on the author's very extensive and valuable PhD research (defended in 2018) and, thus, aims to provide an in-depth scientific study of a particular legal phenomenon: the right to erasure (Art. 17 GDPR). The book appears in the publication series "*Oxford Data Protection and Privacy Law*", edited by Christopher Kuner and Graham Greenleaf, both of whom can certainly be considered influential figures in data protection law. The aim of said series is to illustrate a wide range of important data protection issues, referring to diverse areas of law such as EU law, comparative law, human rights law, etc. The work is preceded by a foreword by Paul Nemitz, a further well-known data protection expert and Principal Adviser at the European Commission.

Data protection law serves multiple goals. As often happens in law and in real life, the perspective adopted is decisive here. From the perspective of businesses or data controllers, data protection law mainly serves as a legal basis to justify their data processing activities. In his book, Ausloos devotes his attention to the perspective of the individual, or rather, in the terminology of the GDPR: the data subject. From the perspective of data subjects, the regulatory framework of the GDPR can be perceived as a defensive protection shield, contributing to a feeling of safety for data subjects. But Ausloos identifies and il-

¹⁷ *ibid*, 235.

DOI: 10.21552/edpl/2020/3/18

* Axel Freiherr von dem Bussche is Partner at Taylor Wessing. He heads up the Technology, Media & Telecoms practice group and coordinates Taylor Wessing's international US Group for Germany. For Correspondence: <A.Bussche@taylorwessing.com>

luminates another function of data protection law, namely its possible use as an individually empowering instrument for proactive defence. In the author's view, there is a subordinated relationship between the individual and business enterprises in our modern digital economic order. There is an asymmetry of power in favour of the latter. Progressive digitalization has led to a loss of the autonomy, dignity, and freedom of the individual, especially with regard to personal data and privacy. Technology increasingly infiltrates the everyday life of all of us and, thus, makes us dependent, as one cannot just entirely refrain from technology and digitalization. A position of dependence is always also a position of weakness.

In reaction to this, the author dedicates his research to the purpose of working out a legal instrument with which an individual can restore the balance in his or her relationship with data controllers, or rather establish such balance in the first place. Ausloos concludes that ideally, a sound legal framework would counterbalance that asymmetry of power by itself, and without further need for individual action. However, as regards the GDPR, the balance is established by granting more power to the individual and this is done through data subject's rights. Subsequently, ways to safeguard the lost values by virtue of GDPR data subject rights are investigated and illustrated. Ausloos does that by way of example, with a main focus on one of the GDPR core rights, the right to erasure as stipulated in Art. 17 GDPR. He proceeds in a three-step process, asking three questions:

What is the rationale of the right to erasure and when does it apply? If it applies, how to balance rights, freedoms, and interests when accommodating the right to erasure? If the right applies and if a balance is found, what are the practical challenges to realizing the right to erasure and how might they be overcome?

This three-step approach also reflects the whole structure of the book, which is divided in three main parts as well, accompanied by further sub-chapters. In Part I, the author first identifies the concrete scope of the application of Art. 17 GDPR, focusing essentially on its meaning and purpose as a point of departure for further research and the legal origins in European fundamental and constitutional rights. In this context, the author advocates for a functional and granular approach in order to determine the scope of application of the GDPR. While this con-

tributes to the flexibility and responsiveness of the law, it also leads to a dilution of the scope and issues of legal certainty. After presenting the prerequisites and limits of applicability, the manner in which the right is to be applied in order to counteract power asymmetries is discussed in Part II of the book. Here, the focus lies on the necessity of balancing interests, which is inherent in the right to privacy as well as fundamental rights and liberties in general. Not only the obvious balancing of interests with regard to the parties directly involved in the data processing, thus, data subject and data controller is examined. With the same degree of detail and depth as it is maintained throughout the entire book, the author also looks beyond the horizon and does not forget to include the interests of third parties as well as common public interests, which must also be weighed against the privacy interests of data subjects. Ausloos concludes that the GDPR is a self-contained system which itself determines all necessary conditions for fair balancing.

Finally, the author establishes a connection to practice in Part III, as the obstacles to practical implementation of his developed theoretical approaches are evaluated. Here Ausloos considers both the interplay and conflict of the GDPR with other legal frameworks as well as technical limits and possibilities. Both points only become apparent when law is applied in reality. Even though the emphasis on practical relevance lies in the last part of the book, the practical relevance of the author's scientific investigation is established right at the beginning, in the first chapter already. Here the author draws vignettes using real cases from practice (Uber Vignette, Facebook Vignette, Google Vignette, Apple Vignette) to which reference is made repeatedly.

However, the general question accompanying the entire book is whether and how the rights granted by the GDPR to data subjects can be applied effectively as a tool to counteract *power asymmetries* and enforce *individual empowerment*. Consequently, to a certain extent the title of the book does not do justice to the material scope and depth of the work, as it suggests that the author's research and work is limited to Art. 17 GDPR, which is only partially true. Not until the fourth chapter will this particular right be dealt with in great depth and detail. Ultimately, however, the author comes to the specific conclusion in his evaluation with regard to Art. 17 that the Right to Erasure does indeed contribute to self-determination

or individual empowerment and the balance of power, but unsurprisingly does not represent a panacea for the challenges of the digital society. Law is not perfect. However, two important functions of Art. 17 are identified, namely the concretisation of the control imperative of Art. 8 of the Charter of Fundamental Rights as well as ex-post compliance control of particular data processing (because if Art. 17 can be successfully made fruitful, obviously something went wrong).

Although recognising the special relationship of the GDPR to Art. 8 of the European Charter of Fundamental Rights, which the author repeatedly mentions at given points, Ausloos pleads for the recognition of the autonomous status and function of the GDPR to, irrespective of the fundamental right to data protection of Art. 8. For the GDPR serves as a means of securing many other rights and freedoms, and thus, according to the author, a restriction to Art. 8 does little justice to it.

It is noteworthy that in the course of the work, new or revolutionary approaches and ideas do not really come to light, as is often the case with PhD theses in particular. This was explicitly not the author's ambition for the work and research. Rather, in the context of his book, Ausloos develops a kind of detailed instruction manual on how to deal with the data subject rights in the light of individual empowerment. However, this is done solely on the basis of the existing legal framework, which as such is not questioned or excessively criticized but rather only *applied* carefully and thoughtfully. This is not an attempt to overturn the law, but rather to confirm it. A systematic overview of the legal and factual situation is given and subsequently an attempt to bring structure and order into the complexity of individual data protection law enforcement is made. Therefore, a new function of the GDPR and a new approach to the rights of the persons concerned are indeed presented, but without having to use methods of legal development or design.

The examination of the individual rules of this still very young field of law offers a deep dive insight in-

to the *raison d'être* of data protection law as such. The author has chosen a very relevant topic, namely the rights of data subjects, the tensions between individuals and companies and Art. 17 GDPR in particular, all of which have been of equal concern to academic experts, practitioners and jurisprudence since the GDPR came into force in 2018. This is also a subject-matter which does not merely touch upon data protection law on the surface or is limited to a rare special problem of mainly academic nature.

Rather, the work concerns the essence of data protection law itself, and is therefore of omnipresent relevance, also in practice. After all, what is more important in practice than the enforcement of claims by stakeholders against the addressees of the regulation? Through the fundamental work that Ausloos has done here, the book may serve as a guide for lawyers of all spectrums. As technology keeps developing rapidly, the way in which data subjects can retain sovereignty over their data will continue to be the driving question of the legislators of the future, since the emergence and growth of data protection is inherently tied to technical developments as the author rightly notes by himself.

Finally, a glance at the bibliography, which runs almost to 50 pages, confirms how deeply the author has dealt with the subject matter. The effort that has been put into research is remarkable, but it has also led to scientifically highly valuable work. However, it is somewhat regrettable that no literature was referred to which was published after the applicability of the GDPR in mid-2018. This would have further increased the practical relevance of the work and would have contributed to its topicality and authenticity.

To sum up, Ausloo's most recent publication is a profound, extremely differentiated and self-reflective analysis of a legal phenomenon that originates from a still unexplored field of law. In this way, the author makes a considerable contribution to facilitate the handling of the law at a very early stage – comparably extensive studies on data protection law are rarely found.