

Reinventing data protection? Serge Gutwirth et al., Springer 2009

Btihadj Ajana

Published online: 25 August 2009

© The Author(s) 2009. This article is published with open access at Springerlink.com

Like many normative concepts that have managed to secure a place within the EU Charter of Fundamental Rights, “data protection” has recently become the subject of renewed interest and growing attention from a wide range of fields and disciplines. In light of the ongoing developments in information and communication technology, various debates have been initiated to address the question as to whether the concept of data protection is in need of an urgent revamp if not even entire reinvention. These debates are often driven by a sense of dissatisfaction and trepidation over the current treatment of data protection and its associated concepts. More specifically, they are concerned with the tangible discrepancy existing between the present ‘practice’ and ‘regulation’ of data protection, and the core ‘values’ and ‘principles’ attached to it. The book *Reinventing Data Protection?*, as its evocative and interrogatory title suggests, is indeed one example of such concerns and discussions. Drawing mainly, but not solely, upon the legal perspective, the collection of articles presented in this book aims to provide a full length assessment of the myriad challenges currently facing the notion of data protection and offer a speculative account on the kind of future that lies in store for fundamental rights in general. Additionally, and perhaps more importantly, *Reinventing Data Protection?* also represents an attempt to devise, tentatively at least, a viable normative framework for re-imagining and enacting a new wave of data protection legislation that is both reflective of and stemming from fundamental democratic ideals.

From the outset, a clear and coherent case is formulated *vis-à-vis* the rationale and the driving forces behind the inauguration of such debate. These range from the imperative to identify the most salient ethical values pertaining to the issue of data

B. Ajana (✉)
London School of Economics, London, UK
e-mail: b.ajana@lse.ac.uk

protection, to the need for rethinking the existing legislation and thereby inventing new approaches, fresh instruments and harmonised standards for dealing with the rising challenges of the global networked world. The book divides into four sections, each of which tackles a specific area of the debate, providing an interesting and constructive blend of different yet interrelated arguments and inquiries.

The first part of the book is devoted to discussing ‘fundamental concepts’ that are pertinent to the issue of data protection. Of particular importance in this section is the contribution made by De Hert and Gutwirth with regard to the need for safeguarding, in practice rather than merely in principle, the conceptual and legal *distinction* between privacy and data protection. Drawing on the case law of Strasbourg and Luxemburg, the authors demonstrate that despite the constitutional inclusion of data protection in the EU 2000 Charter of Fundamental Rights, this principle has not yet managed to achieve its full status in action. They therefore argue for a ‘transformative constitution’ that is capable of realising the right to data protection and preventing its occlusion by other rights, such as that of privacy. In a similar vein, Rodotà also examines this distinction and its normative implications *vis-à-vis* democracy and society at large all the while tracing the path of evolution that has led to the recognition of data protection *as* a fundamental right. Whilst this recognition is certainly a promising achievement in its own right, more has yet to be done at both the political and the legal level, according to Rodotà, to optimise the ‘inherent potential’ of the right to data protection and to save it from possible erosion by security and market logic. To this end, the author proposes a conceivable, though preliminary, approach for achieving such goals. In his article, Brownsword adds another dimension to the debate by invoking the notion of consent and its relation to data protection law, particularly in the context of information and communication technologies. In so doing, he introduces further distinctions to demarcate between ‘an informational privacy right’, ‘a right of informational confidence’, and ‘a set of rights covering the ICT-enabled processing of personal data’ (Brownsword, 2009: 109). Tautological or not, these demarcations serve the purpose of emphasising the need to avoid the conflation between the interest in privacy and the interest in the fair processing of personal data while taking into account the individual and contextual scope of each as well as the importance of consent to the preservation of these informational rights. Contrary to the distinctions made by the abovementioned authors between privacy and data protection, Rouvroy and Pouillet argue for a framework whereby these principles are treated as ‘one unique’ goal rather than separate regimes. They regard the distinction made between the two as merely artificial and one that risks ‘obscuring the essential relation existing between privacy and data protection and further estrange data protection from the fundamental values of human dignity and individual autonomy’ (Rouvroy and Pouillet, 2009: 74). In this sense, creating a synthesis between the two concepts is considered as a necessary and beneficial strategy for enabling the automatic capacities of the human subject for self-development and self-determination. The final input in this section is made by Dinant and covers the themes of identity and identifiability in the context of various technologies that are considered as symbolic of the so-called “information society”. Dinant’s main argument revolves around the question of compliance regarding privacy requirements and the kind of regulatory framework needed to fill the gaps in existing data protection legislation.

The second part of the book moves on to briefly address the issue of actors who are involved in data protection. It begins with a chapter by Berkvens which looks at the role of trade associations in making data protection amenable to negotiation between enterprises and consumers. The second chapter by Hustinx considers the role of data protection authorities and makes some recommendations for improving the effectiveness of these entities and reconciling the disjuncture between the principle of data protection and its practice in reality. The third and last chapter tackles the role of citizens as actors in data protection, building on the results of a survey conducted with Dutch, Flemish and English students. It concludes with an emphasis on the need for heightening citizens' awareness of data collection and use, and strengthening existing rules and regulation.

Regulation is indeed the core theme of the third part of the volume. This section extends the previous ones by probing deeper into the regulatory issues concerning consent, actors and the viability of a global model of data protection. As a starting point, Bygrave and Schatrum explore the notion of consent from the vantage point of decision-making at the operative level (development and application of concrete information systems). Their aim is twofold: first, they attempt to provide a critique of the way in which consent is framed and articulated in current data protection law, namely as being a solitary, individuated, and independent action. Against this, and as a second objective, Bygrave and Schatrum propose an alternative view whereby consent can be perceived and performed 'collectively' rather than individually. Remaining within the macro approach towards data protection, de Terwangne asks the question as to whether a global regulatory model is possible. According to the author, whilst there is a marked worldwide expansion of awareness regarding the issue of data protection, there still remains a need to enrich the fundamental principles of data protection with additional ones in order to redress and maintain a balance between the efficiency of data processing and the rights and interests of data subjects. Another issue of particular pertinence to data protection is that of technical standards. In her article, Winn looks at the ways in which the development and implementation of good ICT standards can contribute to the enhancement of privacy and the effectiveness of data protection regulation. For Winn, this can be achieved through a clear distinction between social and economic regulation so as to delineate the appropriate technical qualities as well as the necessary political accountability for building a robust data protection regulatory system. In the last article of this section, Raab and Koops contribute with a policy actor-based approach to data protection as a means of complementing the predominant tools-oriented analysis. While the latter is useful in clarifying the 'how' and 'what' of information privacy protection, the authors argue that it is not sufficient for understating the challenges of data protection in that it does not address the 'who' dimension, i.e. the actors. As a response, Raab and Koops embarked on the task of mapping the landscape of the wide range of actors involved in the realm of privacy and data protection while identifying some of their interconnections and interrelations.

The final and most extensive part of the book engages with a cluster of issues, most of which are normatively geared towards the future of data protection and privacy. The question of whether a 'common' approach to data protection is needed at the pan-European level is the key theme of Blas' and Nouwt's articles. Blas contends that whilst it is important to ensure the compatibility of rules adopted

across Member States, establishing a general framework with catch-all provisions runs the risk of creating unregulated areas as well as uncertainty, and disregarding the specificity of the manifold categories of data subjects. Nouwt, on the other hand, favours the adoption of a general EU-wide approach to the extent that he sees the latter as capable of guaranteeing a fair processing of data by both governments and industries, not only at the national level but also at the international one. This idea of a common approach to data protection places the notion of accountability centre stage. In considering the present legal standards relating to international data flows, Kruner criticises their existing ‘adequacy’ framework calling for an accountability-based approach instead. Accordingly, this approach would require the allocation of liability to a party based in the EU in order to ensure the presence of a responsible entity to which individuals and authorities can turn when problems with data protection emerge. Given its strong association with surveillance and data mining activities, the issue of profiling is another relevant topic of inquiry. In her article, Hildebrandt provides a cogent assessment of the impact of profiling technologies on data protection and personal autonomy, exploring some ways of rethinking the legal status of the profile to empower citizens and safeguard their rights. The remaining chapters in this section focus mainly on the issue of privacy. They provide a reflection on the challenges and conflicts existing within the domain of privacy advocacy (Hosein), on the nature of the relationship between freedom of information/expression and privacy (Szekely), and on the ways in which risk management processes, especially those concerning the networked activities of the Internet, can affect privacy and inform its regulation (Trudel).

Overall, this volume offers an interesting and balanced account of what has become of the concept of data protection since its inclusion in the 2000 Charter of Fundamental Rights. In engaging with the technological challenges of the networked world as well as the limitations of existing legislations, this collection constitutes a useful companion for legal experts in the field and newcomers alike. What is particularly compelling about *Reinventing Data Protection?* is its constructive character which takes us beyond the disabling cynicism, that is currently circulating amid some debates and discussions, towards more proactive suggestions that promise a positive change in the way in which the principles of privacy and data protection are approached, conceptualised and enacted. But whether these suggestions are amenable to implementation and realisation, is of course something that remains to be seen. What also remains to be seen is whether legislative interventions of this kind are sufficient to support the work needed to restore and protect the myriad values and rights orbiting around the category of the ‘human’. It might be that the urgent task is not so much providing answers, but asking *more* questions.

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.