German Law Journal (2020), **21**, pp. 80–84
doi:10.1017/glj.2019.100

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Delivering Data Protection: The Next Chapter

Orla Lynskey*

> *[I]n the light of the objective … of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively.*[1]

The right to data protection set out in Article 8 of the EU Charter of Fundamental Rights had played a pioneering role in the development of EU fundamental rights jurisprudence. *Schecke and Eifert* became the first to deal a fatal blow to specific legislative provisions that were deemed incompatible with the Charter requirements.[2] *Digital Rights Ireland* led to the annulment of an entire legislative instrument on the same basis.[3] Moreover, in *Schrems*, the Court elaborated on the essence of the related right to respect for private life, indicating that it was this level of fundamental rights protection that served as the benchmark to assess the adequacy of the data protection offered by third countries.[4] Writing in an extra-curial capacity, Koen Lenaerts, President of the Court of Justice of the EU, considered this to be another first. In *Schrems*, the CJEU declared for the first time that an EU measure was invalid on the ground that it did not respect the essence of two fundamental rights—for example, the right to respect private life and the right to effective judicial protection.[5]

This role for the Charter in the metamorphosis of EU data protection law from niche regulatory framework to lodestar in the EU's fundamental rights acquis stood in stark contrast to the role that the Charter had played in lending life to other rights. Chalmers and Trotter suggested, with reference to the sovereign debt crisis, that the transformative effects of the Charter were over-stated. Their claim was that the Charter situated, and protected, individuals within the European political economy while excluding those outside this sphere—for instance, the economically inactive.[6] In this way, it failed to offer protection in situations of great need, such as when individuals were isolated and vulnerable. From a comparative perspective, it was unsurprising therefore that data protection had been likened to the US First Amendment,[7] the jewel in the crown of the EU's Bill of Rights, with its expansion deemed "unstoppable."[8]

*Associate Professor of Law, LSE; Visiting Professor, College of Europe Bruges.

[1]Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317, Judgment of 13 May 2014, at para. 53.

[2]*See* EJC, Joined Cases C-92/09 & 93/09, Volker und Markus Schecke GhbR and Hartmut Eifert v. Land Hessen, ECLI:EU:C:2010:662, Judgment of 9 Nov. 2010.

[3]*See* EJC, Joined Cases C-293/12 & 594/12, Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238, Judgment of 8 Apr. 2014.

[4]EJC, Case 362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650, Judgment of 6 Oct. 2016.

[5]*See* Koen Lenaerts, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, 20 GERMAN L.J., 782, 779–93 (2019).

[6]*See* Damian Chalmers & Sarah Trotter, *Fundamental Rights and Legal Wrongs: The Two Sides of the Same EU Coin*, 22 EUR. L.J. 9 (2016).

[7]*See* Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J 140–54 (2019).

[8]*See* Maja Brkan, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?* 23 MAASTRICHT J. EUR. & COMP. L. 812 (2016).

In practice, the Court had brought the Charter right to bear in data protection judgments by anchoring its interpretation of relevant secondary law instruments—previously the Data Protection Directive, and now the GDPR[9]—in the EU Charter. *Schrems* provided a good example of this. The Court in *Schrems* was asked to interpret a legislative provision that enabled the European Commission to determine whether a non-EU country offered an "adequate" level of rights protection to individuals. The Court considered this provision of the 1995 Directive to have "implement[ed] the express obligation laid down in Article 8(1) of the Charter to protect personal data."[10] While acknowledging that "adequate" protection could not be equated to identical protection, it went on to interpret "adequate" as "essentially equivalent."[11] Such a strict interpretation of "adequate," departing from its ordinary meaning, was facilitated by the invocation of the Charter, which in this instance elevated provisions of secondary law to expressions of a fundamental right.

This judgement, and the Court's subsequent Opinion on the international agreement, concluded by the EU and Canada for the transfer of airline Passenger Name Record (PNR) data, raised difficult practical questions for the EU Institutions. Azoulai and van der Sluis remarked that what is missing in the Court's approach in *Schrems* was "a sense of strategy about the manner in which the Commission can act effectively on the international level."[12] Kuner noted that the quandary the EU Institutions faced when negotiating international agreements was that they needed to meet the very exacting and prescriptive standards which the Court extrapolated from the EU Charter. Yet, third countries might be unwilling to enter into agreements with the EU that may later be picked apart by the Court. Thus, "the unilateral assertion of EU fundamental rights on the international stage m[ight] lead to less rather than more data protection in practice."[13] Of course, the Court's objective in *Schrems* and *Opinion 1/15*—to ensure that the high level of protection provided by EU law was not circumvented by data transfers beyond the EU—was a laudable one. Bridging the gap between a high level of protection on paper and effectively delivering such data protection was, however, difficult.

A similar dynamic was evident in the way in which core concepts—the building blocks—of EU data protection had been interpreted broadly to expand its scope of application while exceptions to its scope had been narrowly construed. This approach—which was evident in judgements concerning the personal,[14] material,[15] and territorial[16] scope—strove to ensure the "effective and complete protection" of EU residents. Again, whether or not the approach adopted by the Court facilitated or detracted from this ambition was contested, the gap between theory and practice persists and conceptual cracks were beginning to appear.

[9]*See* Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC), *repealed by* Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1 (EU).

[10]*Schrems*, Case C-362/14 at para. 72.

[11]*Schrems*, Case C-362/14 at para. 73.

[12]Loic Azoulai & Marijn van der Sluis, *Institutionalizing Personal Data Protection in Times of Global Institutional Distrust*: Schrems, 53 Common Mkt. L. Rev. 1343, 1366 (2016).

[13]Christopher Kuner, *International Agreements, Data Protection and EU Fundamental Rights on the International Stage*: Opinion 1/15, *EU-Canada PNR*, 55 Common Mkt. L.Rev. 857, 882 (2018).

[14]*E.g.*, EJC, Case C-434/16, Peter Nowak v. Data Protection Commissioner, ECLI:EU:C:2017:994, Judgment of 20 Dec. 2017; Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, Judgment of 19 Oct. 2016.

[15]*See* EJC, Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vol; Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388, Judgment of 5 June 2018; EJC, Case C-40/17, Fashion ID GmbH & Co. KG, ECLI:EU:C:2019:629, Judgment of 29 July 2019.

[16]*See Google Spain*, Case C-131/12; *Wirtschaftsakademie Schleswig-Holstein*, Case C-210/16.

https://doi.org/10.1017/glj.2019.100 Published online by Cambridge University Press

So far, however, the Court has not been faced with the practical implications of such a sweeping definitional approach ....[17]

Data protection risked becoming "The Law of Everything," according to Purtova.[18] Mapping the Court's expansive interpretation of "personal data," Purtova cautioned that in circumstances "where all data is personal and triggers data protection, a highly intensive and non-scalable regime of rights and obligations that results from the GDPR could not be upheld in a meaningful way."[19] While this depiction of data protection and interpretation of its jurisprudence was contested,[20] similar misgivings about how best to secure effective data protection were arising from within the Court. When asked to opine upon the application of the data protection rules—and in particular whether a website embedding a piece of Facebook code should be deemed a "data controller"—Advocate General Bobek queried: "Will effective protection be enhanced if everyone is made responsible for ensuring it?."[21] He pointed to the deep "moral and practical dilemma" at the heart of data protection law. The Court has, on the one hand, been inclusive in its definition of the term "data controller" in a bid to secure effective data protection while, on the other hand, it had not been "faced with the practical implications of such a sweeping definitional approach."[22]

The concerns about the Court's expansive approach were two-fold. The first set of concerns were of a practical nature. For instance, it had led to concerns about how the legal framework's general scheme of obligations could apply to existing business models. For instance, in *Google Spain* the Court interpreted the concept of data controller literally to include Google's search engine within its scope. Its stated goal was to ensure the effective and complete protection of fundamental rights. On the contrary, Advocate General Szpunar had subsequently indicated that the provisions of data protection legislation "d[id] not lend themselves to an intuitive and purely literal application to such search engines."[23] Rather, he proposed a rejection of such an "all or nothing" approach in favor of an interpretation of the rules that took into account the "responsibilities, powers and capabilities" of the data controller.[24] This "solution" was implicitly supported by the Court in its judgement.[25] Thus, it seemed that even within the Court, the broad application of the rules was being circumvented through the development of a bespoke application of the regime to specific business models. Whether this approach itself ensured more effective data protection is highly questionable.

At a more systemic and conceptual level, the Court's strict interpretation of the data protection framework risked losing sight of its initial objectives, in particular its capacity to reduce power and information asymmetries between ordinary citizens and those who control the processing of their personal data. The Court's caselaw interpreting the notion of "data controller" provided a good example of this. The application of the Court's findings led to counter-intuitive conclusions—for instance, that an individual data subject can be a data controller in relation to their personal data on the blockchain.[26] Similarly, the attribution of data controller status to each actor operating in the

[17]Opinion of Advocate General Bobek at para. 72, Case C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV (Dec. 19, 2018).

[18]*See* Nadezdha Purtova, *The Law of Everything: Broad Concept of Personal Data and the Future of EU Data Protection Law*, 10 L., Innovation & Tech. 40 (2018).

[19]*Id.* at 42.

[20]*See* Damian Clifford, The Legal Limits of Online Emotional Monetisation paras. 197–99 (June 27, 2019) (unpublished PhD Thesis, University of Leuven) (on file with KU Leuven CiTiP).

[21]Opinion of Advocate General Bobek, *supra* note 17, at para. 55.

[22]Opinion of Advocate General Bobek, *supra* note 17, at para. 72.

[23]*See* Opinion of Advocate General Szpunar at para. 44, C-136/17, G.C. and others v. CNIL, ECLI:EU:C:2019:14 (10 Jan. 2019).

[24]*Id.* at paras. 45, 53.

[25]*See* EJC, Case C-136/17, G.C. and others v. CNIL, ECLI:EU:C:2019:773, Judgment of 24 Sep. 2019 at paras. 47–48.

[26]*See* Lillian Edwards et al., *Data Subjects as Data Controllers: A Fashion(able) Concept?*, Internet Pol'y Rev. (2019), https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400.

https://doi.org/10.1017/glj.2019.100 Published online by Cambridge University Press

data processing chain decoupled these processing operations from the processing system as a whole. The result of this "phase oriented approach to the governance of data processing operations" was that data controller responsibilities, such as transparency, could not be meaningfully discharged and we failed to acknowledge that the effects on individuals were "as a whole – much bigger than the mere sum of the risks connected to the individual processing phases."[27]

In the Court's defense, it was necessary to acknowledge that the text of the GDPR had rendered the task of ensuring its conceptual coherence more difficult. The GDPR integrated the Court's case-law on issues such as territorial scope and added more detail to the obligations and rights it contained. The GDPR also introduced a new layer of data protection meta-regulation, including an accountability mechanism and accompanying provisions on data protection impact assessments and data protection officers, amongst others.[28] There was the hope, of course, that this added layer of regulation will foster greater compliance by ensuring data protection permeated the organizational structures of data controllers and by facilitating the work of supervisory authorities. Although, there was also the risk that this "Byzantine turn"[29] in EU data protection law will simply lead to "formalistic overkill alongside a lack of substantive change."[30]

How then, in the words of Cohen, could we prevent data protection from becoming a form of Kabuki theatre, that distracted users and regulators from what is really going on?[31] Cohen herself pointed to a potential pathway when she suggested that privacy needed to be turned inside out by foregrounding the material and social conditions in which data processing operations took place and decentering the individual in such operations.[32] EU law had the tools at its disposal to turn data protection inside out, albeit perhaps not in distinct ways, to those envisaged by Cohen. The vehicles to facilitate this alternative journey were both internal and external to data protection law.

From an external perspective, the challenge of foregrounding the conditions in which data processing took place had been approached by paying more attention to the environment in which data processing takes place. The ongoing dialogue initiated by the European Data Protection Supervisor concerning digital dominance was an example of this. Implicit in this dialogue was the understanding that the environment in which data protection law applied directly affected its possibilities of success. Unlike regulation, competition law did not seek to design markets yet. Competition law interventions did shape markets and made assumptions about how they work. For instance, between 2008 and 2018, a facilitating mergers and acquisitions regime has enabled Google to acquire 168 companies; Facebook to acquire 71 companies and Amazon to acquire 60 companies.[33] Whether these mergers constituted "killer" acquisitions, which had the object or effect of stymying nascent competition was a question for competition law. By consolidating a greater volume and variety of user data in the hands of a small number of unavoidable actors, however, the environmental changes enabled by competition law also have an effect on data protection.

From an internal perspective, the core principles of data protection law set out in Article 5 GDPR offer an opportunity to shape the data processing environment, and to shift away from the individual-centric approach crystalized in other parts of the GDPR. As has been noted, these principles were "an appealing set of substantive and procedural protections against the power of data intensive companies," which when taken together, "create barriers to big data driven business

[27]René Mahieu & Joris von Hoboken, *Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?*, Eur. L. Blog (2019), https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/.

[28]*See* Reuben Binns, *Data Protection Impact Assessments: a Meta-Regulatory Approach*, 7 Int'l. Data Priv. L. 22 (2017).

[29]*See* Lee Bygrave, Keynote Address at Tilburg University Conference, TILTing Perspectives 2019, *Data Protection = PDF*, (May 15-17, 2019), https://www.tilburguniversity.edu/research/institutes-and-research-groups/tilt/events/tilting-perspectives/keynote-speakers.

[30]Lillian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, 16 Duke L. & Tech. Rev. 80, 18–81 (2017).

[31]*See* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 Phil. & Tech. 8, 1–19 (2018).

[32]*See* Julie E. Cohen, *Turning Privacy Inside Out*, 20 Theoretical Inquiries L. 1 (2019).

[33]*See* Elena Argentesi et al., Ex-post Assessment of Merger Control Decisions in Digital Markets: Final Report 149, 1–164 (2019).

https://doi.org/10.1017/glj.2019.100 Published online by Cambridge University Press

models."[34] Indeed, there had been renewed scholarly attention to these principles. Recent work has been shedding light on the principle of "fairness" in data protection law,[35] and calling for the rejuvenation of the principle of data minimization.[36]

These principles were therefore a potent yet under-utilized resource, which could be drawn upon by the Court to bring about dramatic changes to the data processing environment. Although these core principles had remained intact and largely untouched since the earlier 1995 Directive, they had not yet been applied to great avail in EU data protection law. A good example of this was the failure, to date, of EU data protection law to impose any meaningful constraints on the collection of personal data in the context of content and services that are provided "for free" at the point of access. In 2011, the Irish Data Protection Commission concluded that it could not invoke data protection law to require Facebook-Ireland to "deliver a free service from which members can have the right to opt-out completely from the means of funding it."[37] Some personal data processing was arguably necessary in such transactions. Yet the question remains: How much data processing is necessary? The principle of data minimization, according to which personal data processing should be limited to a minimum in relation to its stated purpose, might be instructive in this regard. This "necessity" element was mirrored in Article 7(4) GDPR. This article provided that when considering whether consent to personal data processing is freely given, it should be taken into account whether the execution of a contract was made conditional on consent to unnecessary processing. A lot will therefore hinge on the interpretation of *necessity*: A broad interpretation of necessity will do little to incentivize a change in current data processing practices, which are designed to extract and extrapolate as much as possible from users, while a narrow interpretation could force to data controllers to rethink the design and funding of their business models.

Early indications from the Court suggest that it may be reluctant to look under the hood of data processing practices and business models and to parse the meaning of necessity. In his Opinion in *Planet49*, Advocate General Szpunar accepted that the underlying purpose of an online lottery—in which users could participate if they agreed to marketing contacts from a minimum of 30 commercial partners—was "the 'selling' of personal data."[38] He opined that the processing of personal data was necessary for participation in the lottery as the provision of personal data constituted the main obligation on the user in order to participate in the lottery.[39] The Court did not adjudicate on this element of the case.[40] One must hope, however, that in the future it brought this limitation on bundling and the principle of data minimization to life in this context.

While EU Charter rights were "less attentive to the singularity, vulnerability and potential of human existence," they were more attuned to the complexities of modern market excesses "and the stresses and demands posed for individuals by these market processes."[41] The real test for the EU Charter right to data protection will be to see whether it could disrupt exploitative business models and practices. The alternative was that data protection becomes part of the problem—a legitimizing framework for exploitative processing practices. We can only hope that the Court will opt for a truly pioneering way to deliver data protection.

[34]Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means* 28 Info. & Comm. Tech. L. 77, 65–98 (2019).

[35]*E.g.*, Jef Ausloos and Damian Clifford, *Data Protection and the Role of Fairness* 37 Yearbook Euro. L. 130–87 (2018).

[36]*See* Mireille Hildebrandt, *Primitives of Legal Protection in the Era of Data-Driven Platforms*, 2 Geo. L. Tech. Rev. 252 (2018).

[37]Data Protection Commissioner, Facebook-Ireland Ltd: Report of Audit 44 (2011).

[38]Opinion of Advocate General Szpunar, supra note 23, at para. 99.

[39]Opinion of Advocate General Szpunar, supra note 23, at para. 99

[40]Opinion of Advocate General Szpunar, supra note 23, at para. 64.

[41]Damian Chalmers & Sarah Trotter, *Fundamental Rights and Legal Wrong*, 22 Eur. L.J. 9 (2016).

Cite this article: Lynskey O (2020). Delivering Data Protection: The Next Chapter. *German Law Journal* **21**, 80–84. https://doi.org/10.1017/glj.2019.100