This is a pre-publication version of Granger, M.-P., and Irion, K. (2018). 'The right to protection of personal data: the new posterchild of European Union citizenship?' in: de Vries, S., de Waele, H., and Granger, M.-P., eds., *Civil Rights and EU Citizenship* (Cheltenham: Edward Elgar Pub.), DOI: 10.4337/9781788113441.00019

11. The right to the protection of personal data: the new posterchild of European Union citizenship?

Marie-Pierre Granger and Kristina Irion

1. Introduction – The 'model' trajectory of the right to data protection and the development of European Union citizenship

Like European Union (EU) citizenship, the right to the protection of personal data is rooted in market integration. It has however quickly taken a life of its own, and now firmly follows a rights-focused trajectory. Formally speaking, the right to the protection of personal data is not a EU citizenship right. It is not listed in Article 20 TFEU and Chapter V of the EU Charter of Fundamental Rights (CFR, or 'Charter') on citizens' rights. The EU institutions and bodies nonetheless treat the right to data protection as an important right of EU citizens. This is clearly visible in Advocate General Da Cruz Vilalon's conclusion in the *Digital Rights Ireland* case, as he stated that 'the collection and… the retention…of the large quantities of data generated or processed in connection with most of the everyday electronic communications of *citizens of the Union* constitute a serious interference with the privacy of *those* individuals.'[1] The EU Commissioner Vera Jourova recently stressed that the data protection reform 'strengthens *citizens*' rights',[2] and the European Parliament (EP) presented it as 'put[ing] the *citizen* back in the driving seat'.[3] Moreover, the Article 29 Working Party guidelines explain that data protection authorities will focus their work on 'claims where there is a clear link between the data subject and the EU, for instance where the data subject is a *citizen* or *resident* of an EU Member State.'[4] The right to data protection may not be a EU citizenship right *stricto sensu*, but it certainly qualifies as a fundamental right of EU citizens, and belongs to the core EU values protected under Article 2 TEU, and which define EU citizenship.[5]

[1] Advocate General Opinion in cases C-293/12 *Digital Rights Ireland* and C-594/12 *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* ECLI:EU:C:2013:845 (emphasis added).
[2] E.g. Vera Jourova, 'How does the data protection reform strengthen citizens' rights' (emphasis added), Factsheet, January 2016, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404; EU Fundamental Rights Agency, 'Information society, Privacy and Data Protection', at http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection accessed 24 Nov 2017.
[3] European Parliament, 'Q&A: new EU rules on data protection put the citizen back in the driving seat', Press Release, 17 December 2015, (emphasis added), http://www.europarl.europa.eu/pdfs/news/expert/background/20160413BKG22980/20160413BKG22980_en.pdf accessed 24 Nov 2017.
[4] Article 29 Data Protection Working Party, 'Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/121 - WP225,' adopted on 26 November 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (emphasis added), accessed Nov 27, 2017.
[5] European Commission (2017), '2017 Report on EU citizenship – Strengthening citizens right in a Union of democratic change', http://europa.eu/rapid/press-release_IP-17-118_en.htm, accessed 24 November 2017.

Personal data is peculiar in the way it brings the dignity of a human being together with valuable economic properties.[6] Like silkworms producing a raw silk thread to make a luxury cloth, [7] individuals generate a personal data trail as a by-product of their multifarious online activities, which largely exceeds the personal information they actively volunteer in online transactions. Thanks to the 'smart' everything - from phones to watches, household appliances, cars and cities - our movements and activities get registered, even when we are offline. What used to be the exclusive domain of governments - surveillance - has become regular business. This new 'surveillance capitalism' uses data to 'predict and modify human behavior … to produce revenue and market control.'[8]

Since the 1990s, the EU, mobilized by various institutional and civil society actors, has sought to tame public and private appetites for personal data and to subjugate their use to principles and procedures. The protection of personal data is nowadays guaranteed by an effective combination of various EU legal instruments, notably the EU Treaties, the EU Charter, and secondary EU legislation. It offers a legal and institutional framework which is unparalleled in other parts of the world, and which protects not only nationals of Member States but also Third Country Nationals who can demonstrate some connection with the EU (e.g through residence).[9]

In this chapter, we argue that the right to data protection is the posterchild of EU citizenship in the digital era. We start by providing a brief overview of the gradual construction of the right to personal data protection in the EU. We then identify a range of actors who have played a particular role in the construction process, including EU citizens themselves. Next, we review the current legal 'architecture' of the right to the protection of personal data and discuss whether it could serve as a model for the future development of EU citizenship, notwithstanding remaining challenges at the level of national implementation and public and private compliance with EU rules. Finally, we reflect on the future development of the right to data protection, and its contribution to the development of EU citizenship as a legal regime.

2. The gradual construction of the right to personal data protection: new EU citizens' rights for the new digital age

Over the years, the right to personal data protection has evolved from a market building device into a core EU fundamental rights, and arguably, a de facto EU citizenship right. Initial EU legislation ensuring protection to personal data in the context of market integration has been extended to other areas of activities and further reinforced by constitutional recognition, which attributes to this right a particularly strong position in the EU legal order.

2.1 Born as internal market legislation

Whilst originating in the internal market, the protection of personal data was infused from the beginning with human rights considerations, which influenced its later development. Indeed, in response to the first wave of automated data processing, in 1995, the predecessor of the

[6] Beate Roessler, 'Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspective* (Cambridge: Cambridge University Press 2015).

[7] Analogy adapted from Chris Marsden and Ian Brown, *Regulating Code: Good Governance and Better Regulation in the Information Age* (Cambridge MA: MIT Press, 2013).

[8] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 *Journal of Information Technology* 75 http://dx.doi.org/10.1057/jit.2015.5 accessed 24 November 2017.

[9] See Article 29 Data Protection Working Party (above n 4).

EU, the European Community, adopted the first major legislative instrument: the Data Protection Directive.[10] Based on the EU competence to approximate member states' laws in order to ensure the realization of internal market objectives,[11] the Directive's official purpose was to ease the mobility of personal data across EU borders. It nonetheless also invoked the right to privacy as a general principle of Community law, deriving from the constitutions and laws of the member states and the European Convention on Human Rights (ECHR).[12] Its recital indeed made it clear that 'data-processing systems are designed to serve man …[and] must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals'.[13] The twin purpose of the Directive, to guarantee both the free movement of personal data and the protection of individuals' fundamental rights, has been regularly emphasized by the Court of Justice of the European Union (CJEU).[14] The Luxembourg-based court has significantly contributed to developing the right to the protection of personal data, in particular where it also contributed to facilitating critical intra-EU data flows.[15]

The Data Protection Directive applied to a whole range of activities involving the processing of personal data in both the public and private sectors, thus ensuring a broad scope of protection.[16] However, it excluded police and justice cooperation, or national security. In 2008, the EU adopted legislation which sought to ensure the protection of personal data when these are transferred in the context of cooperation between member states' authorities in those policy areas.[17] The processing of personal data by EU institutions and bodies themselves is, for its part, governed by a separate Regulation, which is equivalent in substance to the Data Protection Directive.[18] These various legislative instrument are, nowadays, complemented by, and embedded in, a robust constitutional right.

2.2 A free standing constitutional right

The growth of data processing since the turn of the century, and in particular the increased volume, variety and velocity of 'big data' applications and resulting data collection and movement, called for an upgrade in the degree and level of protection at European level. The

[10] Directive 95/46/EC 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]OJ L 28/31.
[11] Now Article 114 TFEU.
[12] Kristina Irion, 'A Special Regard: The Court of Justice and the Fundamental Rights to Privacy and Data Protection' in Ulrich Faber et al (eds), *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte* (Nomos 2016) p. 873; Elise Muir, 'The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges' (2014) 51 *Common Market Law Review* 219.
[13] Data Protection Directive, Recital 2 (n 10).
[14] See CJEU, joined cases C-465/00, C-138/01 and C-139/01 *Rech- nungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*, ECLI:EU:*C*:2003:294, para. 70.
[15] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: OUP, 2016).
[16] It is further complemented by sector-specific legislation, such as the E-Privacy Directive, which guarantees, inter alia, communications secrecy (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37.
[17] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350/60.
[18] Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1.

right to personal data protection, now primarily framed as a fundamental right, rather than a market device, has gained a prominent position in the EU constitutional framework.

The right to the protection of personal data made its first significant 'constitutional' appearance in Article 8 of the EU Charter of Fundamental Rights. Drafted in 1999, the Charter codified judge-made general principles for the protection of fundamental rights, and also introduced a few new rights, such as the right to the protection of personal data (Article 8 CFR). After being solemnly proclaimed in 2000, the Charter was eventually granted legally binding force by the Treaty of Lisbon in 2009 (Article 6(1) TEU). It applies to EU institutions and bodies, as well as member states when they implement EU law (Article 51(1) CFR).[19] The 'new' right to personal data protection is 'based' on the Data Protection Directive and ex-Article 286 EC, and is inspired by Article 8 ECHR on the protection of private and family life, as well as the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, ratified by all EU Member States.[20] Article 8 CFR is an atypical provision in many respects. First of all, it provides for an autonomous right to the protection of personal data, separate from the right to privacy. This is distinctive of the EU approach to data protection, and the full implications of this emancipation of data protection are yet to be explored.[21] Second, it prescribes an institutional requirement of supervision by an 'independent authority', which entrenches continued and professionalized data privacy bodies in the EU and could prevent cross-border flows of personal data to countries which do not provide sufficient institutional guarantees.

In addition to the Charter provision, the Treaty of Lisbon also introduced special data protection provisions into the EU treaties. Article 16 TFEU establishes the right to personal data protection, as its first paragraph replicates the wording of Article 8 CFR. In its second paragraph, it lays down a legal basis which empowers EU institutions to adopt 'rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data'. It reasserts that respect for the protection of personal data must be ensured by dedicated independent authorities. Article 16 TFEU belongs to Title II 'Provisions of general application', which confirms its general importance across all EU areas of activities. It is complemented by Article 39 TEU, which provides for guarantees for the protection of personal data in the separate context of the Common Foreign and Security Policy.

The multiple inclusion of the right to data protection in the EU primary law since Lisbon confers it a solid constitutional status. The effect is already perceptible in institutional practices. For example, the CJEUs' balancing act when interpreting the Data Protection Directive has visibly tipped in favor of an 'effective and complete protection of the fundamental rights and freedoms of natural persons'[22] and 'a high level of protection.'[23] The successful invocation of the 'constitutionalized' right to data protection in litigation before

[19] For official clarifications on the scope of application of the Charter, see Praesidium of the Convention on the Future of Europe, 'Explanations relating to the Charter of Fundamental Rights' (2007/C 303/02), OJ [2007] 303/17, 32. This was confirmed in C-617/10 *Åklagaren v Hans Åkerberg Fransson* ECLI:EU:C:2013:105, para 19-21.

[20] See Explanations, ibid., 20.

[21] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Vol 16 (Springer 2014); Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 *International and Comparative Law Quarterly* 569.

[22] 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, para. 53.

[23] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, para. 39.

EU and national courts against not only national but also EU intrusive measures, such as the Data Retention Directive, EU Commission Safe Harbor Decision) has further reinforced its position in the EU fundamental rights' framework.[24]

2.3 A new generation of legislative instruments: the EU data protection reform

Since the adoption of the 1995 Directive, automated data-processing activities have decupled, due to the significant improvements in data storage and computing capabilities, which underpin contemporary practices, such as 'big data' and 'cloud computing'.[25] Moreover, algorithmic decision-making, machine learning and artificial intelligence are fueling data-driven markets, with serious implications for individuals and society at large. As part of its 2012 Digital Agenda Strategy, the Commission initiated a major reform of the data protection legislative framework.[26] It sought to overcome the persistent fragmentation of the internal market caused by divergent national implementations of the 1995 Directive, to modernize data protection law, and to guarantee a better protection of individuals' fundamental rights.[27]After four years of intense legislative wrangling, the EU legislator adopted the General Data Protection Regulation (GDPR),[28] as well as a new Directive concerning data protection in the context of law enforcement. [29]

The GDPR, as it is known, enters into force in May 2018. By and large, it continues the regulatory approach of the Data Protection Directive but comes with improvements and a few novelties. Probably the most interesting innovation or at least one which possibly has interesting implications for the concept of EU citizenship, concerns the territorial scope of the Regulation. Indeed, the GDRP applies extraterritorially, to protect all individuals located in the EU and whose personal data is gathered in the course of online transactions or in the

[24] Joined cases C-293/12 *Digital Rights Ireland* and C-594/12 *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* ECLI:EU:C:2014:238; *Schrems* ibid. See Marie-Pierre Granger and Kristina Irion 'The Court of Justice and the data retention directive in *Digital Rights Ireland:* Telling off the EU legislator and teaching a lesson in privacy and data protection', (2014) *European Law Review,* 39:4, 835. For a study of the evolution of the right to data protection in EU law, see Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Vol. 16, (Springer, 2014).

[25] Manon Oostveen and Kristina Irion, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in Bakhoum, Conde Gallego, Mackenordt, and Surblyte (eds.), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* (Berlin, Springer, forthcoming), Kristina Irion, 'Your Digital Home Is No Longer Your Castle: How Cloud Computing Transforms the (Legal) Relationship between Individuals and Their Personal Records' (2015) 23 *International Journal of Law and Information Technology* 348.

[26] Kristina Irion and Giacomo Luchetta, *Online Personal Data Processing and the EU Data Protection Reform* (Centre for European Policy Studies 2013), https://www.ceps.eu/publications/online-personal-data-processing-and-eu-data-protection-reform, accessed on 24 November 2017.

[27] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, 'Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century' (COM/2012/09 final) 25 January 2012, Orla Lynskey, 'The "Europeanisation" of Data Protection Law' [2016] *Cambridge Yearbook of European Legal Studies* 1 http://www.journals.cambridge.org/abstract_S152888701600015X accessed 28 Nov, 2017.

[28] Regulation 2016/679/EU 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, and repealing Directive 95/46/EC, known as General Data Protection Regulation (GDPR).

[29] Directive 2016/680/EU 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

context of monitoring their behavior.[30] That way, it ensures the protection of EU citizens and residents from abusive practices from companies operating from outside the EU.[31] Its practical effectiveness remains to be seen thought. Moreover, despite relevant adjustments, the GDPR has been criticized for preserving an outdated logic of linear lifecycles in personal data processing that no longer corresponds with today's capabilities in computing and data analytics.[32]

Like its predecessor, the GDPR applies to both the public and the private sectors, with exceptions for law enforcement and national security activities which fall outside the scope of EU law. The protection of personal data in law enforcement activities is governed by a new Directive, which replace the pre-existing Framework Decision, and which was adopted in parallel to the GDPR. The EU nonetheless missed the opportunity to integrate its own institutions' data processing activities into the general framework, and retains the model of regulation through a separate instrument. The fragmentation that prevailed before the adoption of the GDPR has therefore not disappeared. Member States and private actors are subject to the same general regime, except in matters related to law enforcement, where states are subject to a different framework, and EU institutions and bodies follow their own set of rules (which are nonetheless substantively equivalent).

3. The 'builders' of the right to data protection

The current relatively comprehensive EU system of protection of personal data came about thanks to the effective and successful mobilization of the EU legislators and courts by determined societal actors, including key institutional players, expert groups, civil society organizations and EU citizens themselves. Traditionally, in the EU, the Commission initiates legislation, drafting proposals which it submits to the EU legislator (ie the European Parliament and the Council) for discussion, amendment and adoption. However, more often than not, new EU laws and policies, or reform of existing ones, occur under the impulsion and influence of a broader set of political and societal actors, involving corporate players,[33] expert networks,[34] interest groups[35] or civil society organizations.[36] Moreover, through strategic litigation, organised interests can effectively use the judicial system to raise awareness on a problem and influence the policy agenda, or to secure the development of new rules or favorable interpretation and application of existing rules.[37] In the case of data

[30] GDPR, n 28, Article 3(2). On this, see Merlin Gömann, 'The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement' (2017) 54 *Common Market Law Review* 567; Paul de Hert and Michal Czerniawski, 'Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context' (2016) 6 *International Data Privacy Law* 230.

[31] Irion and Luchetta (n 26).

[32] Ibid., For an analysis, see Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 1.

[33] See David Coen, 'The evolution of the large firm as a political actor in the European Union' (1997) 4:1 *Journal of European Public Policy* 91.

[34] E.g. Anthony Zito, 'Epistemic communities, collective entrepreneurship and European integration' (2001) 8:4 *Journal of European Public Policy* 585; Claudio Radaelli, 'The public policy of the European Union: Whither politics of expertise?' (1999) 6:5 *Journal of European Public Policy* 757-774.

[35] See Sonia Mazey and Jeremy John Richardson (eds) *Lobbying in the European Community* (Oxford: Oxford University Press, 1993).

[36] See Sophie Jacquot and Tomaso Vitale, 'Law as weapon of the weak? A comparative analysis of legal mobilization by Roma and women's groups at the European level' (2014) 21:4 *Journal of European Public Policy* 587.

[37] See Christopher Harding, 'Who Goes to Court in Europe? An Analysis of Litigation Against the European Community (1992) 17:1 *European Law Review* 104; Christopher Harding, Utta Kohl and Naomi Salmon, *Human Rights in the Market Place: The Exploitation of Rights Protection by economic actors* (Aldershot:

protection in the EU, an epistemic community of data privacy experts effectively lobbied an initially reluctant Commission to harmonize the protection of personal data in Europe, monitor respect for EU data protection rules, and ensure their adaptation to new challenges. The EU framework was further consolidated through litigation activities. Here, not only organized interests (e.g. corporations, NGOs), but also concerned and affected EU citizens themselves, actively mobilized courts at national and EU level, to flesh out the EU protective apparatus or to enforce the right to data protection against the inertia or negligence of national and EU institutions and bodies in the face of growing tendencies of public and private surveillance.[38]

3.1. The adoption and reform of EU data protection legislation: expert communities in action

The construction of the EU legislative framework for data protection resulted primarily from the active mobilization of expert communities. It proceeded in two distinct waves. The first generation was the consequence of the activism of national privacy specialists. The more recent reform was the product of intense negotiations and lobbying, in which data protection specialists from various institutional bodies and elected representations proved influential, countering heavy corporate lobbying.[39]

In the first wave, members from national data privacy authorities, who 'feared that unconstrained technology would threaten the civil liberties of European citizens'[40] and were concerned that market integration would jeopardize protection standards and challenge their regulatory authority, successfully deployed their expertise to push for a protective agenda at EU level.[41] They leveraged both the potential adverse impact of diverse - and for some deficient - national data protection regimes, on the free flow of data across the EU, and the reorientation of the European project towards citizens' rights following the Maastricht Treaty (i.e. EU citizenship, fundamental rights protection) to secure protective harmonizing legislation at EU level.[42]

Ashgate Publishing, 2008); Lisa J. Conant, *Justice contained: law and politics in the European Union*, (Cornell University Press, 2002), Virginie Guiraudon, 'Equality in the making: implementing European non-discrimination law' (2009) 13:5 *Citizenship Studies* 527; Rachel A. Cichowski, *The European court and civil society: litigation, mobilization and governance* (Cambridge: Cambridge University Press, 2007); Uladzislau Belavusau, 'EU sexual citizenship: Sex beyond the internal market' in Dimitry Kochenov (ed.), *EU Citizenship and Federalism: The Role of Rights* (Cambridge: Cambridge University Press, 2017). For an overview of academic work on litigation and legal mobilization more generally, see Michael McCann, 'Litigation and Legal Mobilization', Gregory A. Caldeira, R. Daniel Kelemen, and Keith E. Whittington (Eds.) *The Oxford handbook of law and politics* (Oxford, Oxford University Press, 2008) 522.

[38] Granger and Irion (n 24); Loïc Azoulai and Marijn van der Sluis, 'Institutionalizing Personal Data Protection in Times of Global Institutional Distrust: Schrems' (2016) 53 *Common Market Law Review* 1343; Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press 2008).

[39] The new general data protection was apparently the most lobbied piece of legislation in Europe, see Floris Kreiken, 'The Lobby-Tomy', 18 February 2016, Bits of Freedom, Amsterdam, https://www.bof.nl/wp-content/uploads/20160218_the_lobby_tomy_report.pdf, accessed 24 November 2017; Jan Philipp Albrecht, 'The EU's Data Protection Reform', Brussels, December 2015, https://www.janalbrecht.eu/fileadmin/material/Dokumente/20151211-JPA-Datenschutzreform-ENG-WEB-01.pdf, accessed on 24 November 2017.

[40] Abraham L. Newman, 'Protecting Privacy in Europe: Policy Feedback and Regional Politics' in Sophie Meunier and Kathleen R. McNamara (eds), *The State of the European Union* (Oxford: Oxford University Press 2007) 127.

[41] Abraham L. Newman, 'Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive' (2008) 62 *International Organization* 103., see also Ibid.

[42] Spiros Simitis, 'From the Market to the Polis: The EU Directive on the Protection of Personal Data' (1994-1995) 80 *Iowa Law Review* 445.

The second wave saw a concerted effort from institutional data privacy experts, in the face of intense lobbying from corporate giants.[43] The Article 29 Working Party, which coordinates Member States' data protection authorities, influenced the EU policy process through the timely and targeted release of opinions and interpretative guidelines on existing and future data protection rules. The European Data Protection Supervisor (EDPS), which is the dedicated EU independent supervisory authority, also played an important supporting role. Flagging its mission, which includes that of ensuring that EU institutions' respect the right to personal data protection when they design, adopt and implement policies, it issued numerous critical opinions and statements which influenced the drafting of the reform proposal. The EP rapporteur, acting with other members of the competent parliamentary committee, was also central in defending the protective dimension of the legislative proposal. The Vice-President of the Commission, Viviane Reding, also fought hard against backsliding attempts.[44] The unprecedented lobbying by corporate players or powerful third countries' authorities led many MEPs to react and mobilize in support of privacy rights.[45] During the reform discussions, European Digital Rights (EDRi), the European Consumer Organisation (BEUC) and a few other groups intervened to represent the interests of EU citizens and individuals at large. Being notoriously on the shorter end of resources and womanpower, they nonetheless managed to gain public attention by exposing the extent of corporate lobbying through the publication of a comparison between stakeholder documents and MEPs' tabled amendments.[46] Academics across Europe also released an open statement in support of the data protection.[47] The Snowden revelations in early 2013, and international news media reporting over the reach of mass surveillance by the US National Security Agency, which was seemingly tapping into the personal logs and data of the largest US Internet companies, further fueled mobilization in support of stricter data protection rules.[48]

Whilst expert communities were instrumental in bringing about legislation on data protection and ensuring high protection standards, despite corporate attempt at undermining them, civil society organizations and citizens have effectively mobilized national and EU judicial systems to consolidated EU protection of personal data.

3.2 Creating protective precedent: civil society and citizens' mobilization

[43] David Bernet, *Democracy* (Documentary film, 2015).

[44] E.g. Viviane Reding, 'Vice-President Reding's intervention during Justice Council Press Conference', SPEECH/13/514, 6 June 2013 http://europa.eu/rapid/press-release_SPEECH-13-514_en.htm, accessed on 24 November 2017.

[45] For instance, the US mission had raised issues directly with the Commission even before the official legislative proposals were submitted to the EP (US Mission, "Informal Comment on the Draft General Data Protection Regulation and Draft Directive on Data Protection in Law Enforcement Investigations", 16 January 2012, https://edri.org/files/US_lobbying16012012_0000.pdf; accessed on 24 November 2017). On this, see Sophie in 't Veld, 'EU Data Protection Reform: Lead MEP in 't Veld criticizes undue lobbying by US Authorities', ViEUws The EU Policy Broadcaster, March 14, 2013, http://www.vieuws.eu/citizens-consumers/eu-data-protection-reform-lead-mep-in-t-veld-criticises-undue-lobbying-us-authorities/, accessed on 24 November 2017.

[46] A crowdsourcing platform run by the Berlin-based Open Data City project shows which amendments were proposed by lobbies and submitted as such verbatim by MEPs, but also visualizes how the member states voted in the Council (www.lobbyplag.eu).

[47] Academic signatories, 'Data protection in Europe: Academics are taking a position," (2013) 29 *Computer Law & Security Review* 180.

[48] Glenn Greenwald, 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian*, 7 June 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed 24 November 2017; G. Günter Frankenberg, *Political technology and the erosion of the rule of law: normalizing the state of exception* (Cheltenham: Edgar Elger, 2014); Kristina Irion, 'Accountability Unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection' in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds), *Privacy in the modern age: the search for solutions* (The New Press 2015) 78.

Courts are reactive and contingent institutions, deciding on questions about the interpretation and application of the law, in the context of disputes which are submitted to them by public and private litigants.[49] They can, to some extent, 'control' their docket, by showing more or less sympathy towards certain kinds of claims, and open the door wider to particular claimants.[50] In the case of data protection, the CJEU has displayed a welcoming and encouraging approach, which contribute to further reinforce the protective EU framework.

The Court's 'special regard' for the right to the protection of personal data is revealed by a range of indicators and anecdotal evidence.[51] First, the well above average frequency with which the Court sits as a 'Grand Chamber' in data protection cases signals their importance in the eyes of the Luxembourg judges. Second, the unusual readiness with which the Court annulled EU acts found to disproportionately restrict the right protected by Articles 8 CFR, also suggests that data protection is 'different' from other rights,[52] for which the Court has shown greater deference to EU law-makers.[53] Finally, the quality and rigor of the Court's reasoning in data protection cases, which contrasts with the brusque manner in which it sometimes brushes away other human rights arguments,[54] suggests there is a strong consensus within the Court in support of that cause.[55]

The development and enforcement of the EU regime of personal data protection is, moreover, supported by favorable legal opportunities in some member states, such as legal standing for NGOs, or the possibility of collective claims, which have encouraged EU law based litigation and provided material and opportunities for the CJEU to mold protective principles. It also benefits from a strong societal vigilance, perhaps rooted in European authoritarian pasts. For example, after the adoption of the Data Retention Directive, 34 000 German citizens filed separate actions against the national implementation measures, and obtained from the German Constitutional Court that it strikes them down.[56] In the meanwhile, the Irish organization 'Digital Rights Ireland', as well as an Austrian local government and more than 11 000 Austrian citizens brought separate actions before domestic courts against domestic implementation measures. The case was referred to the CJEU, which invalidated the controversial EU measure, and took the opportunity to lay down the ground rules for national data retention regimes.[57] This visibly encouraged data privacy defenders to contest other EU measures. In 2016, *Digital Rights Ireland*, and *La Quadrature du Net*, a French digital rights group, filed separate actions against the 'EU-US Privacy Shield', an arrangement which succeeds the Safe Harbour agreement, invalidated by the Court in *Schrems I,*[58] to facilitate

[49] Austin Sarat 'The litigation explosion, access to justice, and court reform: Examining the critical assumptions' (1984) 37 *Rutgers Law Review* 319, 325-326.
[50] On the role of legal opportunity structures, see Christopher Hilson 'New social movements: the role of legal opportunity' (2002) 9:2 *Journal of European Public Policy* 238, 243.
[51] Irion (n 12).
[52] Granger and Irion (n 24).
[53] See Andrew Williams, *EU Human Rights Policies: A Study in Irony,* (Oxford: Oxford University Press, 2004).
[54] Ibid.
[55] Rumor even has it that the *Schrems* ruling of 6 October 2015 was delivered only two weeks after Advocate General Bot delivered his Opinion to allow President Vassilios Skouris to take part in the ruling before his term ended.
[56] Federal Constitutional Court of Germany, 'Data retention unconstitutional in its present form', Press Release No. 11/2010 of 2 March 2010, http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html accessed 28 November 2017.
[57] Digital Rights Ireland (n 24).
[58] Schrems I (n 23).

the transfer of personal data from the EU to the US.[59] The same year, Maximilian Schrems, an Austrian law student now turned 'legal entrepreneur', brought an action which challenges the Commission's decision on EU-US data transfer channels used by Facebook, in which he represents the interests of more than 25 000 'consumers' (*Schrems III*).[60] With the entry into force of the GDPR, public interest groups will have the right to represent the interests of 'data subjects' (Article 80), mirroring similar provisions in EU environmental and consumer protection law. The relaxation of standing rules for NGOs should result in further data protection litigation.

EU and national data protection authorities also play an important role in the judicial development and enforcement of EU data protection law. The EDPS has managed to secure broad participation rights in the CJEU, which it has used to influence case law developments. Indeed, the original mandate of the EDPS granted the office holder the right to intervene in proceedings concerning data processing by EU institutions and bodies. However, in the Passenger Name Records (PNR) cases, which concerned measures allowing for the transfer of the personal information of air transport passengers, the EDPS claimed a right to intervene in direct actions (e.g. annulment actions, infringement proceedings) which have implications on data protection, which the CJEU granted.[61] In preliminary reference proceedings (Article 267 TFEU), which make up the bulk of the CJEU case law and through which it most significantly contributes to the development and enforcement of EU data protection rules, the CJEU has developed a practice of asking the EDPS to provide expert opinions, based on Article 24 of the Court's Statute.[62] The EDPS has actively taken up this new role, pleading for the enhanced recognition of data protection as a fundamental right and an important value in EU law.[63] Its expertise, and position in the EU institutional framework, contributes to its influence on the shaping of EU data protection law.

In sum, the increased frequency with which the CJEU rules on data protection is not only a reaction to contemporary challenges in the digital environment, but is also the result of the Court's welcoming approach to privacy concerns. This, in turn, has empowered and emboldened organizations fighting for greater informational privacy across the EU, as well as individual citizens concerned by intrusive surveillance practices, who called upon EU law and the Court to uphold protective standards. The resulting growing number of references, and the variety of questions raised, has given the Court the opportunity to make significant principled contributions on data protection standards. It has also offered the Court a unique opportunity to boost its own legitimacy and expand its review powers. In the process, it has positioned itself as a champion in a field of increased relevance to EU citizens, and has shown it could live up to its constitutional mandate of protection of fundamental rights.[64]

---

[59] General Court, case T-670/16 (*Digital Rights Ireland v Commission*) and case T-738/16 (*La Quadrature du Net and Others v Commission*), both pending.

[60] Austrian High Court, Decision about the reference to the CJEU, 6 Ob 23/16z (*Maximilian Schrems v. Facebook Ireland Ltd.*), 20 July 2016, http://www.europe-v-facebook.org/sk/OGH_Vorlage.pdf, accessed on 24 November 2017.

[61] Order in Case C-317/04, *European Parliament v Council of the European Union*, ECLI:EU:C:2005:189.

[62] Protocol No 3 on the Statute of the Court of Justice of the European Union, Consolidated Version, https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-08/tra-doc-en-div-c-0000-2016-201606984-05_00.pdf, accessed on 24 November 2017.

[63] EDPS, 'Pleading before the Court of Justice Case C-362/14, *Schrems v Data Protection Commissioner'*, Luxemburg, 24 March 2015, https://edps.europa.eu/sites/edp/files/publication/15-03-24_edps_pleading_schrems_vs_data_commissioner_en.pdf, and 'Public hearing in Joint Cases C-239/12 and C-594/12 (9 July 2013) Pleading of the EDPS', Luxemburg, 9 July 2013, https://edps.europa.eu/sites/edp/files/publication/13-07-09_pleading_notes_joint_cases_c-23912_and_c-59412_en.pdf, accessed on 24 November 2017.

[64] Irion (n 12).

Still, despite the mobilization of citizens and civil society, data protection authorities and the support of important EU institutions, the development of data protection rules suffers from a corporate bias, in the sense that litigation targets primarily state measures and not corporate practices. This results both from features of EU law and the nature of societal concerns. First, provisions of EU Directives, such as the Data Protection Directive, have only vertical direct effect: when non (properly) implemented, they can be invoked in courts only against emanations of the state, but not against private parties.[65] This may explain why the EU case law, fueled by preliminary references from national courts, concerned mostly violations of the right to personal data resulting from public actors' activities or omissions, and not from those of corporations. Moreover, citizens' vigilance and mobilization of the judicial system seems stronger in the case of state surveillance, as citizens worry about public authorities' intrusion into their private life, whilst they are resigned over corporations turning their personal data into a counter-performance in exchange for access to services, in the context of e-commerce, social networks, or other internet-based services.[66] Still, despite some deficiencies, the EU system of data protection is a robust one, which could be emulated to promote and protect other important fundamental rights of EU citizens.

4. The legal 'architecture' of the right to the protection of personal data – a possible model for the effective protection of EU citizens' civil liberties?

The architecture of the right to the protection of personal data is a relatively solid one, with two strong constitutional pillars, and an extensive legislative framework. The articulation of the different legal instruments is complex, but makes for an interesting set up. Indeed, despite some substantive overlap and repetition, the Regulation-Treaty-Charter triptych appears like an good recipe to ensure the protection of data privacy in the EU against intrusions from both public and private actors.

The coming into force of the GDPR carries important implications. First of all, as an EU Regulation, it is directly applicable (Article 288 TFEU). This feature does away with problems related to delayed, incomplete or incorrect transposition of EU Directives. Second, it imposes direct and clearer obligations on both public and private actors. Third, it makes the EU dimension of the protective legislation more visible, and with it, the associated requirement of effective judicial protection (Article 19(1) TEU and Article 47 CFR). Finally, and foremost, unlike the Directive, it produces direct horizontal effect, and can thus be invoked in litigation against both public and private actors. It thus increases the potential exposure of private actors and may contribute to refocusing litigation towards intrusive practices by corporate actors, rather than just public bodies.

Moreover, Treaty recognition can contribute to the development of a more robust and consistent approach to data protection across a broad range of activities. Indeed, EU Treaty provisions can produce both vertical and horizontal direct effects, meaning that they can be relied on in domestic litigation against both state and private actors.[67] The formulation of

[65] On the vertical direct effect of the Directive, see case 41/74, *Yvonne van Duyn v Home Office* ECLI:EU:C:1974:133. On the lack of horizontal direct effect of the Directive, see case 152/84 *M. H. Marshall* v *Southampton and South-West Hampshire Area Health Authority (Teaching)* ECLI:EU:C:1986:84.

[66] In relation to the collection of fingerprints for obtaining travel documents, see Henri de Waele, 'Access to travel documents', 8 September 2016, Deliverable D.7.6 of the bEUcitizen project: https://doi.org/10.5281/zenodo.61783, 21-30. On concerns related to the retention of traffic data, see Marie-Pierre Granger and Orsolya Salat, 'Report exploring the mechanisms for enforcing civil rights with a view to identifying the barriers', Deliverable D7.2 on the bEUcitizen project, 2 March 2016, https://doi.org/10.5281/zenodo.46835 (both accessed on 24 November 2017), 22-39.

[67] On the vertical and horizontal direct effect of Treaty provisions, see case 26/62 *NV Algemene Transporten Expeditie Onderneming van Gend en Loos v. Nederlandse Administratie der Belastingen* ECLI:EU:C:1963:1

Article 16 TFEU appears sufficiently clear and precise to produce direct effect.[68] Its wording stands the comparison with Article 21 TFEU which guarantees EU citizens' right to free movement, and which the CJEU recognized as directly effective.[69] In any case, following the *Mangold/Kücükdeveci* line of reasoning,[70] developed in the context of age discrimination, like data protection characterized by the presence of specific Treaty provisions and strong legislative instruments, one could also argue for the recognition of a general principle for the protection of personal data, which could be invoked against public and private actors where EU legislation reaches its limits.[71] The horizontal effect of Charter provisions, such as Article 8, is still an open question,[72] but loses some of its relevance when the right protected by a Charter provision (like Article 8 CFR) is also embedded in Treaty provisions, general principles and legislative provisions which themselves can be applied in horizontal disputes. The (potential) recognition of the right of data protection as a directly effective primary EU law norm offers a stronger guarantee that all public and private authorities are subject to similar obligations, irrespective of whether their activities fall under the scope of the GDPR or other instruments, and should support the more coherent development of EU data protection law.

In a manner similar to the EU equal treatment and non-discrimination framework, the articulation and complementarity between the different legal instruments which guarantee the right to the protection of personal data in the EU offer an interesting model for the future of the protection of EU citizens' civil rights, such as, for example, the right to a fair trial or freedom of expression. Indeed, under the 'regular' Charter scheme, individuals can only invoke Charter provisions 'when Member States are implementing EU law' (Article 51(1) FCR), a notion which is interpreted by EU (and national) courts in a restrictive and inconsistent manner, and which prevents citizens from relying on the EU Charter and activating EU law remedies against violations of their Charter rights which do not fall within the scope of EU law so defined.[73]

5. 'Maintenance work' – the constant challenge of enforcement and compliance

Whilst the EU has pieced together a comprehensive framework for the protection of personal data, its implementation and practical application still pose problem. The political science literature on Europeanization and EU compliance has identified various factors that affect compliance with EU rules. These include notably the compatibility between existing national

---

and case 43/75 *Defrenne* v *SABENA*, ECLI:EU:C:1976:56. For a detailed study of the effect of EU Directives, see Sacha Prechal, 'Directives in European Community law: A study of directives and their enforcement in national courts' (Oxford: Clarendon Press, 1995).

[68] *Van Gend en Loos* ibid. for an argument to this effect, see Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?' (2009) 46 *Common Market Law Review* 1485.

[69] The CJEU ruled in relation to Article 18 EC, the predecessor of Article 21 TFEU. See case C-413/99 *Baumbast and R v Secretary of State for the Home Department* ECLI:EU:C:2002:493, para 84.

[70] See case C-144/04 *Werner Mangold v Rüdiger Helm ECLI*:EU:*C*:2005:709; C-555/07 - *Kücükdeveci ECLI*:EU:C:2010:21.

[71] Muir (n 12). Alan Dashwood, 'From *Van Duyn* to *Mangold* via *Marshall*: Reducing Direct Effect to Absurdity?' (2007) 9 *Cambridge Yearbook of European Legal Studies* 81.

[72] Case C-176/12 A*ssociation de médiation sociale* v *Union locale des syndicats CGT and Others* ECLI:EU:C:2014:2.

[73] Eleonora Spaventa, 'The interpretation of article 51 of the EU charter of fundamental rights: The dilemna of stricter or broader application of the Charter to national measures (Study for the PETI Committee)' PE 556.930, February 2016, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556930/IPOL_U(2016)556930_EN.pdf, accessed on 24 November 2017.

laws and EU norms ('goodness of fit'), the 'quality' of EU legislation (its clarity and precision), the participation of stakeholders in the EU law-making and implementation process, or the EU enforcement capacity, as well as a range of domestic legal and political factors (e.g. the openness, quality and effective functioning of the national judicial systems in relation to EU based claims; administrative capacity; support or opposition of domestic political actors, etc.).[74] Many of these factors are relevant to the specific context of ensuring public and private actors' compliance with EU rules for the protection of personal data. Moreover, data protection law is complex, subject to fast-moving technological developments and involving significant profits, which further hampers the effectiveness of an otherwise strong protection system. The incorporation of the right into EU primary law and the adoption of the GDPR can help address some of the enforcement challenges, but difficulties which are both classic implementation problems, and others more peculiar to the field of data protection are likely to remain.

The Commission's reports on the implementation of the 1995 Data Protection Directive,[75] the impact assessment which preceded the recent reform of the EU data protection regulatory framework,[76] and research on threats to civil rights arising in the context of the implementation of the EU Data Protection instruments,[77] suggest that the Directive not only failed to achieve its internal market harmonization objective, but also suffered from significant enforcement problems. The Commission identified a number of shortcomings. Some concern the EU instruments themselves, which sometimes do not provide for sufficiently precise or adequate definitions, as well as the way public and private actors (ab)use of the lee-way they have to apply EU rules in a manner which defies the protective aim of the Directive. Particular problems arose in relation to the definition of personal data (e.g. inclusion of IP addresses or geo-location data); the notions of 'controllers' and 'processors' and their respective roles and responsibilities; the definition of 'consent'; the scope of certain exemptions (e.g. 'household exemptions, or freedom of expression); the territorial scope of application of the Directive; the interpretation of key principles of data protection (e.g 'purpose-limitation', 'data minimization', 'transparency' and 'accountability'); the classification of so-called 'sensitive data' (e.g. genetic and biometric or health data, offences and criminal convictions) and the scope of the public interest exception; the nature of the duty to inform data subjects, and the range of rights afforded to them (access, rectification, deletion, withdrawal, etc.); the question of the legality of, and safeguards applicable to, the transfer of data to third countries, and so on.[78]

---

[74] For a review, see Tanja Börzel, and Thomas Risse, 'Europeanization: The domestic impact of European Union politics', Knud Erik Jørgensen, Mark Pollack, Ben Rosamond (eds) *Handbook of European Union Politics* (SAGE, 2007) 483. On compliance, see Gerda Falkner and Oliver Treib, 'Three worlds of compliance or four? The EU-15 compared to new member states' (2008) 46:2 *Journal of Common Market Studies* 293.

[75] Report from the Commission, 'First report on the implementation of the Data Protection Directive (95/46/EC)' COM (2003) 265 final, 15 April 2003; Communication follow-up of the Work programme for a better implementation of the Data Protection Directive, COM (2007) 87 final, 7 March 2007.

[76] Commission Staff Working Paper, 'Impact Assessment, accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' SEC(2012) 72 final, 25 January 2012, Annex 2 Evaluation of the implementation of the Data Protection Directive, at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf, accessed on 24 November 2017.

[77] Granger and Salat (n 66).

[78] Commission Staff Working Pape (n 76).

Furthermore, there are significant problems with administrative and judicial enforcement mechanisms. These appear particularly pronounced where data protection or privacy have not traditionally received prominent protection in the national legal system (e.g. in the United Kingdom), or where administrative and judicial systems are generally deficient (e.g. Hungary).[79] Moreover, there are serious practical challenges. Given the technical expertise (including legal knowledge) required to design and apply compliant data protection policies, and to monitor compliance, public bodies, such as data protection authorities, have an important role to play. They are, however, not always granted sufficient guarantees of independence, investigative or sanctioning powers, or resources, to carry out their tasks effectively.[80] Some contributed significantly to the enforcement of EU data protection rules, and cooperated in the context of joint enforcement actions,[81] but others fail to take on an active role.

Judicial remedies, before either/or administrative and ordinary courts, are generally available. However, the apparent small stakes, and the complexity of the field, which incur important legal expertise costs, probably discourage many individuals from taking violations to court. In this context, NGOs play a fundamental role by actively supporting individual cases, organising collection litigation, or even constructing and bringing cases themselves (like in the *Digital Rights Ireland* case), in particular in taking on corporate giants or public surveillance schemes. Oftentimes, national courts have offered assistance and upheld privacy concerns. They appear ready to stand up to big corporations, but are often more deferential to data collection and use for security purposes by law enforcement bodies, unless these practices are clearly too far reaching (e.g. the 'File of Honest People' in France) and disproportionate to the security objective pursued.[82] Already prior to the invalidation of the Data Retention Directive by the CJEU, a number of national courts had criticized national implementing measures on national constitutional grounds.[83] Eventually, the question came before the CJEU, which annulled it, and imposed strict limitations on national data retention policies.[84] Many national courts followed up by striking down or neutralizing national data retention measures.[85] National legislators nonetheless keep on adopting new amending measures, which still include pre-emptive and blanket data retention, despite the CJEU prohibition. NGOs brought the matter back to the CJEU, which in its recent ruling on the *Tele2/Watson* case, reaffirmed that EU law outlawed 'national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.'[86]

---

[79] Granger and Salat (n 66), 38-39.

[80] See EU Fundamental Rights Agency, 'Data Protection in the European Union: the role of National Data Protection Authorities' (Luxembourg: Publications Office of the European Union, 2010).

[81] Jacob Kohnstamm, 'Getting Our Act Together: European Data Protection Authorities Face Up to Silicon Valley' in Paul de Hert and David Wright (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer International 2016), 455.

[82] Granger and Salat (n 66).

[83] E.g. in Bulgaria, Cyprus, Czech Republic, Germany and Romania. See Ludovica Benedizione and Elenora Paris, 'Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive' (2015) 16 *German Law Journal* 1727; Eleni Kosta 'The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection' (2013) 10 SCRIPTed 339.

[84] Granger and Irion (n 26).

[85] Ludovica Benedizione and Eleonora Paris, 'Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive' (2015)16 *German Law Journal,* 1727.

[86] See Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB, Tom Watson and Others* ECLI:EU:C:2016:970, para. 112.

Until now, sanctions imposed on those who breach EU data protection rules, whether administrative fines or criminal penalties, are not commensurate with the financial benefits derived from the collection, access and use of personal data. The GDPR could alter the cost-benefit calculus and increase the deterrent effect of the EU regime, as it provides for new sanctions amounting to up to four percent of the total worldwide annual turnover of the undertaking.[87]

The reform of the EU data protection framework, and notably the adoption of the GDPR, is supposed to address some of the implementation and enforcement shortcomings, but the complexity of EU data protection law, and practical difficulties in its operationalization will continue to be major factors undermining its effectiveness. Even willing, resourceful and well-advised public bodies, corporate actors or civil society organizations struggle to be fully compliant with the specifications of EU data protection law. These difficulties are further exacerbated by rapid technological change, which leave law and legal procedures oftentimes lagging behind,[88] and the financial benefits and market advantages drawn from undercutting or bending data protection rules. With the adoption of the GDPR, a further challenge will concern the geographical scope of applying the Regulation. Following a 'destination' approach, the Regulation seeks to reinforce the effective protection of EU citizens in the age of the Internet, as data travel across the world faster than the time that it takes to click.[89] Whilst logical from the perspective of the protection of EU citizens' right to data protection, it will inevitably trigger conflicts of laws and jurisdictional issues, and generate controversies related to the legitimacy of the extraterritorial application of EU data protection law.[90]

5. Conclusion: the right to data protection – the new EU citizens' right

Over two decades, the protection of the right to personal data has undergone a radical transformation, mutating from a market supporting device into an autonomous civil right of those who live in the EU, and a core European value. The mixed legal framework which ensures its protection could serve as a model for the future development of EU citizenship, in particular if it is to evolve towards a more rights-based notion, away from its reminiscent market building function.[91] The future of the right to data protection nonetheless faces a number of challenges. It imposes demanding requirements on public and private actors alike, which require access to, and the deployment of, significant human and financial resources not all can afford. These burdensome requirements are not always necessary to secure a sufficient level of protection. The recent reform, notably, failed to address the 'scalability' of protection, as regulatory interventions regulate each single act of processing through rather malleable obligations .[92] Moreover, the strong recognition currently afforded to data protection in the EU raises concerns as to the balance of rights which constitutes the EU constitutional identity. The CJEU has recognized that the fundamental right to data protection is not absolute, that it must be 'considered in relation to its function in society',[93] and

[87] Article 83(5) GDPR.
[88] Granger and Salat (n 66) 38-39.
[89] de Hert and Czerniawski.(n 30).
[90] Ibid.
[91] Marie-Pierre Granger, 'The protection of civil rights and liberties and the transformation of EU citizenship' in Sandra Seubert, Marcel Hoogenboom, Trudie Knijn, Sybe de Vries and Frans van Waarden (eds) *Moving Beyond Barriers – Prospects for EU Citizenship?* (Cheltenham, UK: Edward Elgar, forthcoming).
[92] Irion and Luchetta (n 26).
[93] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR, Hart- mut Eifert v Land Hessen*, ECLI:EU:C:2009:284, para. 48.

reconciled with other fundamental rights.[94] As a matter of fact, the protection of personal data often supports the exercise of other important fundamental rights and values (e.g. freedom of expression),[95] but it can also be (ab)used to limit them (e.g. freedom of information).[96] There is also the risk that the EU right to data protection falls victim of its own success. Indeed, the improved legal opportunity structures for the protection of personal data under EU law, together with the publicity surrounding the coming into force of the GDPR, could trigger a sharp rise in data protection litigation and a massive increase in case referrals to the Luxembourg Court, which may well be tempted to tone down its initial enthusiasm and adopt more restrictive approaches to avoid overload. There is moreover a recent tendency to overcharge EU data protection law with expectations that it would come to terms with the much more complex challenges of algorithmic decision-making and artificial intelligence. Personal data protection regulation is not capable of remedying all negative effects technology can have on personal autonomy and our social fabric. The ongoing transformation from information technology and the Internet are deeper and more profound than the isolated concern about informational privacy.

[94] CJEU, case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Sa- tamedia Oy* ECLI:EU:*C*:2008:727, para. 53.
[95] E.g. C-203/15 and C-698/15*Tele2 Sverige* (n 86), para. 101; see Oostveen and Irion n 25; Ronald J. Krotoszynski, *Privacy Revisited: A Global Perspective on the Right to Be Left Alone* (Oxford: Oxford University Press 2016).
[96] Granger and Salat (n 66), 37-38.