This is an Accepted Manuscript of a book chapter published in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (Hart 2021),
https://www.bloomsburyprofessional.com/uk/data-protection-beyond-borders-9781509940677/

EU Data Protection Law Between Extraterritoriality and Sovereignty

Edoardo Celeste and Federico Fabbrini

I. Introduction

Writing in the *Harvard Law Review* in 1890, leading American jurists Louis Brandeis and Samuel Warren outlined the contours of a new right to privacy conceived as the right to be let alone.[1] Yet, 130 years later – and with the advent of the digital age – privacy is leaving this perimeter and entering new dimensions, with challenges of their own.[2] As the international newspaper *The New York Times* put it in launching "The Privacy Project", a comprehensive months-long endeavor to explore how technology is altering conceptions of individual privacy, the terminology of privacy itself is changing, and crucially new demands connected to privacy are emerging, especially in relation to the protection of personal data.[3]

The European Union (EU) has been at the forefront of the protection of the right to data protection at the global level. The EU is currently endowed with an advanced constitutional and legislative framework for the protection of personal data. Moreover, the European Court of Justice (ECJ) has taken the lead as the most protective privacy court word-wide, developing a case law which has been taken as a model by courts also at the national level. In fact, recently, the EU legal framework for data protection has proved to be resilient also during the Covid-19 health crisis: in the context of the largest pandemic the world experienced in a century, EU data protection law shaped and constrained government initiatives to track and trace individual movements and contacts, confirming the importance that privacy rights play also in a dramatic health scenario.

Among the data privacy rights developed by the ECJ, and now explicitly codified in EU law, one of the most significant and innovative is the right to be forgotten, also known as the right to erasure: this is right enables data subjects to request data controllers, including

[1] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
[2] See Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2015) 28 *Harvard Human Rights Journal* 65.
[3] See James Bennet, 'Opinion: Do You Know What You Have Given Up' *The New York Times* (10 April 2019) <https://www.nytimes.com/2019/04/10/opinion/privacy-project-launch.html> accessed 13 July 2020.

online digital platforms, the erasure of personal data concerning him or her – an entitlement which has grown in importance in the sprawling digital society.

However, the scope of EU data protection law in general, and the right to be forgotten in particular, has been increasingly facing a question of jurisdictional boundaries. Indeed, one of the most debated features of EU data protection law is its capacity to apply beyond the borders of the EU.[4] Moreover, the recent introduction of harsher fines has led many foreign companies to comply with EU data protection law not only in relation to their European business, but on a global scale. Over the past few years, therefore, the scope of EU data protection law not only expanded by virtue of a precise legislative choice, but also as a result of the economic and political influence of the EU – what Anu Bradford defined the 'Brussels effect'.[5]

The chapter maps the legal architecture for the protection of personal data in the EU, examines its resilience in the context of Covid-19 and explores the question of the extraterritorial application of EU data protection law.[6] The chapter explains that there are good arguments for the EU to apply its high data protection standards outside its borders. As data are un-territorial,[7] only a global application of EU data protection law can fully guarantee an effective enforcement of privacy rights. However, the chapter also highlights how such an extraterritorial application of EU data protection law faces challenges, as it may clash with duties of international comity and the need to respect diversity of legal systems, and could ultimately be nullified by contrasting rulings delivered by other courts in other jurisdictions.

As the chapter points out from a comparative perspective, however, this challenge is not unique to the EU legal system. Rather, it emerges in other jurisdictions as well, such as Canada and Australia. In fact, the protection of privacy in the digital age increasingly exposes a tension between efforts by legal systems to impose their high standards of data protection outside their borders – a dynamic which could be regarded as 'imperialist'[8] – and claims by other legal systems to assert their own power over data – a dynamic which one could name 'sovereigntist'.[9] As the article suggests, navigating between the Scylla of imperialism and the Charybdis of sovereigntism will not be an easy task – particularly when claims to control the digital realm are made by authoritarian regimes, which are

[4] See Dan Jerker B Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 *International Data Privacy Law* 226.
[5] Anu Bradford, 'The Brussels Effect' (2012) 107 *Northwestern University Law Review* 1).
[6] See also Federico Fabbrini and Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders' (2020) 21 *German Law Journal* 55, on which this chapter draws.
[7] Jennifer Daskal, 'The Un-Territoriality of Data' [2015] *Yale Law Journal* 326.
[8] See Oxford Learner's Dictionaries, 'Imperialism' (defining imperialism as "1. A system in which one country controls other countries [...], 2. The fact of a powerful country increasing its influence over other countries through business, culture, etc."), <https://www.oxfordlearnersdictionaries.com/definition/american_english/imperialism> accessed 13 July 2020.
[9] *See* Oxford Learner's Dictionaries, 'Sovereignty' (defining sovereignty as "1. Complete power to govern a country. 2. The state of being a country with freedom to govern itself"), <https://www.oxfordlearnersdictionaries.com/definition/english/sovereignty?q=sovereignty> accessed 13 July 2020.

eager to exploit digital technology for their illiberal mission.[10] In this context, greater convergence in the data protection framework of liberal democratic systems worldwide appears as the preferable – albeit far from easy – path to secure privacy in the digital age.

The chapter is structured as follows. Section II presents the EU constitutional framework for data protection and the expanding case law of the ECJ in the field. Section III overviews the resilience of EU data protection law during the Covid-19 pandemic. Section IV analyzes the right to be forgotten afforded to data subjects – originally developed by the ECJ and then codified in EU legislation. Section V illustrates how the EU framework for data protection has progressively extended its reach outside the jurisdiction of the EU, looking in particular at the recent case law of the ECJ in the field of the right to be forgotten and removal of content from online platforms. Section VI, drawing a comparison with other jurisdictions, explores the rationale behind the extraterritorial application of EU data protection law and examines the challenges that this tendency poses. Section VII finally concludes suggesting that transnational cooperation among liberal democratic jurisdictions appears as the preferable path to navigate the emerging tension between data protection imperialism and digital sovereignty and to guarantee an elevate standard of protection of data privacy in the digital age.

II. EU Data Protection Law and Jurisprudence

At the constitutional level, the EU abides by one of the most advanced standards for data privacy worldwide. The EU Charter of Fundamental Rights adopted in 2000 introduced a constitutional recognition of the right to data protection in the EU legal order.[11] Whereas Article 7 of the Charter (entitled "Respect for Private and Family Life") re-affirmed the content of Article 8 of the European Convention on Human Rights, proclaiming that "Everyone has the right to respect for his or her private and family life, home and communications," Article 8 of the Charter (entitled "Protection of Personal Data") introduced a new explicit recognition of the rights to data privacy by stating that

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

[10] See Yi-Zheng Lian, 'Opinion | Where Spying Is the Law' *The New York Times* (13 March 2019) <https://www.nytimes.com/2019/03/13/opinion/china-canada-huawei-spying-espionage-5g.html> accessed 7 December 2019; The White House, 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain' (*The White House*, 15 May 2019) <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/> accessed 1 December 2019; cf. Zak Doffman, 'Trump's Huawei Ban Rejected By New Ruling In Germany' *Forbes* (15 October 2019) <https://www.forbes.com/sites/zakdoffman/2019/10/15/trumps-huawei-ban-rejected-by-surprise-new-report/> accessed 1 December 2019.

[11] See Maria Tzanou, 'Data Protection as a Fundamental Rights Next to Privacy? "Reconstructing" a Not so New Right' (2013) *International Data Privacy Law* 3.

With the entry into force of the Lisbon Treaty in 2009, the Charter has acquired full legal value.[12] Moreover, the Lisbon Treaty introduced another provision confirming the centrality that the rights to data protection now play in the constitutional order of the EU.[13] Pursuant to Article 16 of the Treaty on the Functioning of the EU (TFEU), "Everyone has the right to the protection of personal data concerning them." The same provision empowers the European Parliament with the Council to

> lay down the 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. Compliance with these rules shall be subject to the control of independent authorities.

At the legislative level, then, the EU has been endowed with a comprehensive framework on data protection since the 1990s. The Data Protection Directive, adopted in 1995,[14] introduced a far-reaching obligation for the member states to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data"[15] within their jurisdictions.[16] The principles codified in the Data Protection Directive were then expanded in 2001 to the EU institutions by a Regulation on the protection of individuals with regard to the processing of personal data by EU bodies, offices and agencies,[17] which also established the European Data Protection Supervisor (EDPS).[18] Moreover, selected pieces of EU legislation expanded the protection of data privacy in specific sectors, such as electronic communications,[19] and police and judicial cooperation in criminal matters.[20]

Ultimately, in 2016, the European Parliament and the Council, on the basis of Article 16 TFEU, enacted the General Data Protection Regulation (GDPR),[21] and simultaneously adopted a Directive on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties.[22] The GDPR replaced the Data Protection Directive with measures directly and uniformly binding throughout the member states of the EU, with the aim to provide an even more advanced framework for data protection, updated to the challenges of globalization and rapid technological developments.[23]

---

[12] See also Federico Fabbrini, *Fundamental Rights in Europe* (Oxford University Press 2014).
[13] See also Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009).
[14] Directive 95/46/EC, OJ 1995 L 281/31.
[15] Id., Article 1.
[16] Id., Article 4.
[17] Regulation 45/2001/EC, OJ 2001 L 8/1.
[18] See Hielke Hijmans, 'The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority' (2006) 43 *Common Market Law Review* 1313.
[19] Directive 2002/58/EC, OJ 2002 L 201/37.
[20] Council Framework Decision 2008/977/JHA, OJ 2008 L 350/60.
[21] Regulation (EU) 2016/679, OJ 2016 L 119/1.
[22] Directive (EU) 2016/680, OJ 2016 L 119/89.
[23] See Viviane Reding, 'The Upcoming Data Protection Reform for the European Union' (2011) 1 International Data Privacy Law 3.

At the jurisprudential level, finally, the ECJ through its case law has championed the protection of data protection, wearing with confidence the role of a human rights court.[24] In particular, heavily drawing on the Charter of Fundamental Rights, the ECJ has expanded its prior jurisprudence[25] and enforced a high standard of data privacy protections: 1) vertically, i.e. vis-à-vis the member states; 2) horizontally, i.e. vis-à-vis the EU political branches; as well as 3) diagonally, i.e. vis-à-vis private companies which withhold relevant power in the processing of personal data. First, the ECJ held that Article 8 of the Charter, and Article 16 TFEU, implied a need for data protection authorities to be fully independent and ruled against member states which had failed to secure this objective in their legislation,[26] and set aside national legislation introducing surveillance measures in breach of data protection rights.[27] Second, the ECJ found that Articles 7 and 8 of the Charter provided data subjects with a right to be protected from practices of systematic government surveillance and thus struck down as incompatible with EU primary law both the EU Data Retention Directive, which required the retention of personal data law enforcement purposes,[28] as well as an international agreement concluded between the EU and Canada, which foresaw the collection of passenger name record (PNR) data.[29] Third, the ECJ has also applied a high standard of data protection vis-à-vis tech companies, subjecting IT providers offering services within the EU internal market to EU data protection laws, and expanding the protections afforded to data subjects.[30]

III. EU Data Protection Law and Covid-19

EU data protection law proved to be very resilient also in the context of one of the most dramatic crisis Europe, and indeed the world, ever faced: the recent coronavirus pandemic. The spread of this new, severe acute respiratory syndrome, known also by its medical acronym Covid-19, resulted in the largest pandemic the world has experienced, at least since the 1918 Spanish influenza. Originally emerged in China in winter 2019, the virus has slowly but steadily spread across the globe, leading in the spring 2020 towards unprecedented governments' action in the effort to stop contagions. Across the world, Covid-19 prompted state authorities to impose war-like lock-downs, closing schools, factories, and public facilities, banning the movement of persons, prohibiting public gatherings and requisitioning properties essential to address the health crisis.

---

[24] Federico Fabbrini, 'The EU Charter of Fundamental Rights and the Right to Data Privacy: the EU Court of Justice as a Human Rights Court', in Sybe de Vries et al. (eds.) *The EU Charter of Fundamental Rights as a Binding Instrument* (Hart 2015) 261.

[25] See e.g. Case C-101/01, *Lindqvist* [2003] ECR I-12971 (ruling that the placing of information on the internet constituted processing of personal data wholly or partially by automated means within the meaning of the Data Protection Directive).

[26] Case C-518/07, *Commission v. Germany* [2010] ECR I-1885; and Case C-614/10, *Commission v. Austria*, ECLI:EU:C:2012:631.

[27] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Postoch telestyrelsen* and *Secretary of State v Watson*, ECLI:EU:C:2016:970.

[28] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communication et al* and *Kärtner Landesregierung et al*., ECLI:EU:C:2014:238.

[29] Opinion 1/15, judgment of Jul. 26, 2017, ECLI:EU:C:2017:592.

[30] See also Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 *International Review of Law, Computers & Technology 76.*

In order to map contagions and prevent the further spread of the virus a number of initiatives were proposed to use digital technology to fight back Covid-19. In some countries, such as Taiwan or Israel, the satellite position of mobile phones was used to monitor people's respect of lockdown measures.[31] In Europe, similar measures were seen as fully incompatible with the right to privacy and data protection. Yet, an intense debate has emerged in relation to the adoption of contact-tracing apps. Contact-tracing aims to identify the network of people met by an individual who has been tested positive to the virus. In this way, national health services can contain the further spread of the virus by asking the concerned persons to self-isolate. Contact-tracing is usually conducted manually, but use of mobile apps can make this process more efficient. By resorting to the technologies embedded in a mobile phone, it is possible to have a more accurate overview of the people who entered in close contact with a specific individual. The conundrum in the EU was therefore how to reconcile the possibility to make contact-tracing more efficient with the need to preserve the respect of fundamental rights, and in particular the rights to privacy and data protection.

From an early stage, however, EU data protection law successfully shaped and constrained the type of initiatives that were proposed, and taken, to use contact-tracing apps in the fight against coronavirus. On 15 April 2020, the President of the European Council and the President of the European Commission put forward a joint European Roadmap towards lifting Covid-19 containment measures, which indicated as a strategy toward the lifting of lock-down measures the creation of "a framework for contact tracing [...] which respects data privacy."[32] Moreover, on 16 April 2020, the European Commission adopted comprehensive guidelines on apps supporting the fight against Covid-19 pandemic in relation to data protection.[33] These emphasized the importance of adhering to the EU data protection framework even in the context of the responses to coronavirus. In particular, while the European Commission recognized that contact-tracing apps could be valuable to respond to Covid-19, it stressed that they had to be designed to fully comply with EU data protection law. As such, the Commission required that the installation of the app had to be voluntary, that proper legislation had to be adopted to this end, and that criteria of data minimization had to be put in place, with limitations on the disclosure and access to the data. The Commission stressed that both GDPR and the ePrivacy Directive prohibit the bulk collection, access and storage of health data and location data. Contact tracing apps are only allowed to process proximity data, i.e. information about the likelihood of virus transmission based on the epidemiological distance and duration of contact between two individuals. For this reason, the use of GPS tracking should be prohibited in the EU, while resorting to Bluetooth technology is recommended. Moreover, the Commission reminded the importance of precisely setting the purpose for data use, ensure the security of the data and set precise time-limit on its use, so as to protect the individuals' trust into this instrument. Otherwise, a similar emphasis on the importance of protecting personal data

[31] See Tomas Pueyo, 'Coronavirus: Learning How to Dance' (*Medium*, 28 May 2020) <https://medium.com/@tomaspueyo/coronavirus-learning-how-to-dance-b8420170203e> accessed 13 July 2020; cf. 'Coronavirus: Israel Halts Police Phone Tracking over Privacy Concerns' (*BBC News*, 23 April 2020) <https://www.bbc.com/news/technology-52395886> accessed 13 July 2020.

[32] European Commission, 'Joint European Roadmap towards lifting Covid-19 containment measures', 2020/C 126/01**,** 15 April 2020, 7.

[33] European Commission, 'Guidance on Apps supporting the fight against Covid-19 pandemic in relation to data protection', 16 April 2020, COM(2020)2523 final.

was put also by the European Data Protection Board, which on 21 April 2020 disclosed its guidelines on the use of location data and contract tracing tools in the context of the Covid-19 outbreak.[34]

As a result of these multiple constraints set by the EU institutions as well as by national data protection authorities all member states' initiatives to develop contact-tracing apps turned into small scale exercises, which gained limited traction among the population.[35] The Covid-19 pandemic, therefore, proved the resilience of EU data protection law and its strength even in the context of the most dramatic health crisis Europe and indeed the world faced in a century. In fact, as the Commission pointed out in its first review of the GDPR – published on 24 June 2020, just over two years since its entry into force – the EU data protection framework proved its worth also in the current Covid-19 pandemic and the effort to use digital technology to fight it, because the "GDPR is clear that any restriction must respect the essence of the fundamental rights and freedoms, and be a necessary and proportionate measure in a democratic society to safeguard a public interest, such as public health."[36]

IV. The Right to Be Forgotten

One of the most significant and innovative features of EU data protection law is the recognition of a right to be forgotten. The first step towards the recognition of such a right was taken by the ECJ in May 2014, in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*.[37] The case concerned the interpretation of the Data Protection Directive, which was then applicable in domestic proceedings between Google and the AEPD, the Spanish data protection agency. Pursuant to the application by a Spanish national, the AEDP had required Google to remove from its search engine links to information relating to the applicant, on the account that data protection law applied to it. Google had challenged the administrative decision in Spanish courts, which decided to refer several questions to the ECJ.

In its judgment, the ECJ recognized a new right for data subjects to request removal of on-line content, and, correspondingly, an obligation for the operator of a search engine to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person.[38] As a preliminary matter, the ECJ ruled that a search engine like Google must be classified as a processor and controller of personal data within the

[34] European Data Protection Board, Guidelines 4/2020, 21 April 2020.

[35] See Ryan Browne, 'Why Coronavirus Contact-Tracing Apps Aren't yet the "game Changer" Authorities Hoped They'd Be' (*CNBC*, 3 July 2020) <https://www.cnbc.com/2020/07/03/why-coronavirus-contact-tracing-apps-havent-been-a-game-changer.html> accessed 13 July 2020; see also Dan Sabbagh and Alex Hern, 'UK Abandons Contact-Tracing App for Apple and Google Model' *The Guardian* (18 June 2020) <https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models> accessed 13 July 2020.

[36] European Commission, 'Data Protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation', 24 June 2020, COM(2020)264 final, 3.

[37] Case C-131/12, *Google Spain v APED* [2014] ECLI:EU:C:2014:317.

[38] See for comments on the case: Eleni Frantziou, 'Further Developments in the Right to Be Forgotten' (2014) 14 Human Rights Law Review 761; and Herke Kranenbourg, 'Google and the Right to be Forgotten' (2015) 1 European Data Protection Law review 70.

meaning of the Data Protection Directive.[39] On the substance, then, the ECJ – after recognizing that a name search through Google could provide a "more or less detailed profile of [the data subject]"[40] – held that the operator of a search engine "is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties […], also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful."[41]

The judgment of the ECJ in *Google Spain* opened the door to a full-fledged codification of the right to be forgotten in EU law. The GDPR, in fact, enshrined in Article 17 a "Right to erasure (right to be forgotten)", stating that "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay." The same provision clarifies that the right to erasure applies when: "(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based [...]; (c) the data subject objects to the processing [...] (d) the personal data have been unlawfully processed."

Moreover, pursuant to Article 17(2) GDPR, "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data." While Article 17(3) GDPR indicates that the right to erasure "shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with legal obligations [...] in the public interest" and for a number of other selected reasons related to public health, scientific or historical research and legal defense, the GDPR seemed to follow the ECJ's view that the data subject's right to request the removal of on-line content "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name."[42]

V. Extraterritorial Application of EU Data Protection Law

Over the past few years, the EU framework for data protection has progressively extended its reach outside the jurisdiction of the EU. To begin with, the ECJ has reviewed the standard of data protection existing in third countries to decide whether this was sufficient to authorize the transfer of personal data from the EU to such third country – essentially pressuring the latter to raise its domestic standards to meet the EU benchmark. In the *Schrems*[43] and *Schrems II*[44] judgments, in particular, the ECJ reviewed the adequacy of

[39] *Google Spain* (n 38), at 41.
[40] Id., at 80.
[41] Id., at 88.
[42] Id., at 97.
[43] Case C-362/14, *Schrems* [2015] ECLI:EU:C:2015:650.
[44] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Schrems* [2020]

the US privacy framework with the EU data protection law, and concluded on both occasions that this fell short of EU standards.[45]

In particular, in *Schrems*, delivered in 2015, the ECJ reviewed the European Commission 2000 Safe Harbor decision – which recognized US data protection standards as providing an adequate level of protection, and therefore authorized private companies to transfer data across the Atlantic[46] – and struck that down, ruling that in light of the revelations of US mass surveillance, it appeared that law and practice in force in the US did not ensure an adequate protection of personal data.[47] The ECJ ruling in *Schrems*, which was prompted by a Facebook user disgruntled with the limited protection that his data would receive in the US, forced the EU and the US to renegotiate further guarantees on the protection of personal data – including limitations on the access and use of personal data transferred for national security purposes as well as oversight and redress mechanisms that provide safeguards for those data to be effectively protected against unlawful interference and the risk of abuse – which were codified in a new Commission adequacy decision called Privacy Shield.[48]

However, in the recent *Schrems II*, delivered in 2020, the ECJ ruled that also the 2016 Privacy Shield was incompatible with the rights to privacy and data protection,[49] as well as with the essence of the right to an effective remedy,[50] enshrined in the EU Charter of Fundamental Rights. While in its judgment the ECJ upheld the European Commission decision on standard contractual clauses,[51] which creates a framework for business to business data exchange, it ruled that the level of privacy protection afforded to data subjects in the US was not adequate, given the ongoing ability of US national security services to undertake surveillance operations on the transferred data, and the limited right to judicial recourse against abuse under US law. In its two *Schrems* rulings, therefore, the ECJ leveraged EU data protection law to put incremental pressure on a third country such as the US. In this way, the EU is successfully raising US standards through international negotiations in order to secure unhindered flow of data beyond borders.[52]

Moreover, the ECJ has directly subjected economic operators incorporated outside the EU to EU data protection rules when they deal with data collected within the EU. The point was already made in *Google Spain*: here the ECJ ruled that in light of the objective of EU data protection law "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, [the notion of establishment] cannot be interpreted restrictively"[53] – and therefore concluded that Google, despite being

[45] See also further Maria Tzanou, Chapter 7.

[46] Commission Decision 2000/520, OJ 2000 L 215/7.

[47] See David Cole and Federico Fabbrini, 'Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders' (2016) 14 *International Journal of Constitutional* Law 220.

[48] Commission Implementing Decision (EU) 2016/1250, OJ 2016 L207/1.

[49] *Schrems II*, para 180.

[50] *Schrems II*, para 187.

[51] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46, OJ 2010 L39/5.

[52] *See* David Cole & Federico Fabbrini, 'Transatlantic Negotiations for Transatlantic Rights', in David Cole et al. (eds), *Surveillance, Privacy and Transatlantic Relations* (Hart 2017) 197.

[53] *Google Spain* (n 38) at 53.

incorporated in the US, was subjected to the Data Protection Directive, also because it operated a subsidiary in Spain, which managed advertising on a Spanish-localized search engine. In fact, the GDPR has further expanded this state of affairs,[54] as Article 3(2) (entitled "Territorial Scope") now foresees that "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

The extraterritorial reach of EU data protection law has led to important challenges – notably with regard to the right to be forgotten, as the ECJ has attempted to work out the circumstances when requests to remove online content bound businesses established overseas, and with world-wide effect. In particular, the matter was at the heart of two recent ECJ judgments concerning US companies Google and Facebook. In September 2019, in *Google v. Commission Nationale de l'Informatique et des Libertés (CNIL)*,[55] the ECJ reviewed a sanction imposed on Google by the French data protection authority for failure to remove content worldwide, from all its website domains, in pursuance of a right to be forgotten request.[56] Google had challenged the CNIL sanction claiming that the removal of online content exclusively on the French version of its search engine sufficed. In its ruling, the ECJ – also taking note of the geo-blocking technology put in place by Google[57] – upheld the challenge.

The ECJ admitted that the GDPR objective is "is to guarantee a high level of protection of personal data throughout the [EU]"[58] – and that "a de-referencing carried out on all the versions of a search engine would meet that objective in full."[59] However, the ECJ emphasized that "numerous third States do not recognise the right to de-referencing or have a different approach to that right,"[60] and claimed that it was not apparent from the GDPR that the intent of the EU legislator was "to confer a scope on the rights enshrined in those provisions which would go beyond the territory of the Member States and [...] to impose on an operator [...] like Google [...] a de-referencing obligation which also concerns the national versions of its search engine that do not correspond to the Member States."[61] Hence, the ECJ concluded that

> where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet

[54] See 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*.
[55] Case C-507/17, *Google v. Commission Nationale de l'Informatique et des Libertés (CNIL)* [2019] ECLI:EU:C:2019:772.
[56] See Quinn, Chapter 5
[57] Id., at 42.
[58] Id., at 54.
[59] Id., at 55.
[60] Id., at 59.
[61] Id., at 62.

> user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.[62]

Yet, if *Google v. CNIL* seemed to draw a limit to the extraterritorial effects of the right to be forgotten, the ECJ decision in *Eva Glawischnig-Piesczek v. Facebook* – delivered just a week later, in October 2019[63] – counter-balanced that. Although this case did not explicitly concern the right to be forgotten, it dealt with an analogous problem – namely the question whether a digital platform could be forced to remove world-wide content posted online which was regarded as defamatory. Mrs Eva Glawischnig-Piesczek, an Austrian politician, had obtained a court order to remove insulting language against her posted on Facebook, but the latter had disabled access to the content initially published only in Austria, prompting the applicant to sue for breach of EU data protection law. In its judgment, the ECJ – after discussing the obligations of digital providers under the e-Commerce Directive[64] – examined whether EU law imposed "any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt" vis-à-vis information society services,[65] and ruled that EU law "does not preclude those injunction measures from producing effects worldwide."[66]

While the ECJ cautioned that "in view of the global dimension of electronic commerce, the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level"[67] – and that therefore "[i]t is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules"[68] – the ECJ judgment's consequence was to open the door to Austrian courts to imposing on Facebook obligations "to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law."[69]

VI. The Challenges of Extraterritoriality in Comparative Perspective

The problem of extraterritorial application of domestic laws in the digital realm is not exclusive of the EU. In fact, as Jennifer Daskal has pointed out, there are now an increasing number of cases adjudicated by courts world-wide which raised "critically important questions about the appropriate scope of global injunctions, the future of free speech on the internet and the prospect for harmonization (or not) of rules regulating online content across borders."[70] In particular, other recent disputes involving US technology companies and decided in the jurisdictions of Canada and Australia have vividly exposed the challenges of an extraterritorial effect of data protection law.

---

[62] Id., at 73.
[63] Case C-18/18**,** *Eva Glawischnig-Piesczek v. Facebook* [2019] ECLI:EU:C:2019:821.
[64] Directive 2000/31/EC, OJ 2000 L 178/1.
[65] *Facebook* (n 59), at 49.
[66] Id., at 50.
[67] Id., at 51.
[68] Id., at 52.
[69] Id., at 53.
[70] Jennifer Daskal, 'Google Inc. v. Equustek Solutions Inc.' (2018) 112 *American Journal of International Law* 727.

In 2017, in the case *Google Inc. v. Equustek Solutions Inc.*, the Canadian Supreme Court ordered Google to remove worldwide from its search engine the links to a company's website violating intellectual property rights.[71] Equustek, a Canadian IT company, had sued Google claiming that the search engine had failed to de-list from its browser the websites of a competitor, which had breached Equustek intellectual property rights by misappropriating its trademarks. In June 2017, the Canadian Supreme Court, deciding on the matter on appeal, ruled in favour of Equustek and granted it the sought injunction, ordering Google to delist from its browser worldwide all the websites that harmed Equustek. According to the Court, a global enforcement of the delisting request was necessary to prevent harm to the plaintiff.[72] However, Google subsequently sought an injunction before the US District Court for Northern California to prevent enforcement in the US of the Canadian Supreme Court order as incompatible, among others, with the US First Amendment guaranteeing freedom of speech and principles of international comity. In November 2017, the US District Court granted Google the injunction sought, effectively nullifying the effects of the Canadian Supreme Court ruling in the US.[73] However, despite the favourable ruling of the Californian court, in April 2018, Google was eventually unsuccessful in its claims before the Supreme Court of British Columbia. The Canadian court was adamant about its refusal to consider Google's demand to limit the scope of its delisting order.[74]

Similarly, also in 2017, in the case *X v. Twitter*, the Supreme Court of New South Wales in Australia ordered the Californian company and its Irish subsidiary to remove at global level a series of confidential information posted by a troll.[75] The applicant X lamented the publication of confidential financial information leaked on Twitter by an anonymous troll from various accounts, including one that used the name of the company's CEO. Twitter was initially reluctant to suspend the incriminated accounts, but was eventually ordered by the court to provide the identity of the troll and to remove all illegal contents published online. In contrast to the Canadian Supreme Court in the *Google Inc. v. Equustek Solutions Inc.* case, the Australian court did not consider principles of international comity nor did it carry out a comparative analysis of foreign law on breach of confidence.[76] Yet, in this case too, the Supreme Court of New South Wales did not hesitate to serve an extraterritorial injunction to remedy the detrimental situation of the domestic applicant.

Similarly to the Canadian and Australian courts, both the recent ECJ cases *Google v. CNIL* and *Glawischnig-Piesczek v. Facebook* at first sight leave the door open to a worldwide application of EU law. In *Glawischnig-Piesczek v. Facebook*, such a global effect represented the primary solution proposed by the ECJ, only subject to the respect of international law.[77] In *Google v. CNIL*, as seen in the previous section, the ECJ affirmed that an EU-only form of delisting would suffice. However, espousing the nuanced approach proposed by Advocate General Szpunar,[78] the ECJ also clarified that nothing

[71] *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34, [2017] 1 S.C.R. 824.
[72] See Jeff Berryman, 'Equity in the Age of the Internet: Google Inc. v. Equustek Solutions Inc.' (2019) 31 Intellectual Property Journal 311.
[73] *Google Inc. v. Equustek Solutions Inc*, Case No. 5:17-cv-04207-EJD.
[74] *Equustek Solutions Inc. v. Jack*, 2018 BCSC 610.
[75] *X v Twitter* [2017] NSWSC 1300.
[76] See Michael Douglas, 'Extraterritorial Injunctions Affecting the Internet' (2018) 12 *Journal of Equity* 34.
[77] Id., at 52.
[78] See Opinion of Advocate General Szpunar at 62.

prevents Member States to allow for global dereferencing, if the protection of individual privacy and personal data outweighs the safeguard of other competing rights.[79]

From an EU perspective, such an extraterritorial application of EU law can be explained by the need to ensure an effective protection of fundamental rights and limit the risk of circumvention.[80] The enforcement of the right to be forgotten is exemplary. We now live in a global digital society, which overtakes national boundaries. One's right to data protection may be violated even where a search engine shows a specific result in a country, which is not that of residence of the data subject concerned. In principle, enforcing that right exclusively within the territory of the EU would not make any sense, given the ease with which data can be accessed world-wide. A violation of such right would occur if an individual, for example residing in France, after lawfully requesting to delist specific search results, discovered that those links are still referenced not only in France, but – say – also in Germany or in the US, with no difference. And this consideration implies that – as much as uniform standards of data protection should apply within the EU – EU data protection rights should also have extraterritorial effects outside the EU.

Nevertheless, the extraterritorial application of EU data protection law poses a series of challenges – which were vividly exposed in the *Google Inc. v. Equustek Solutions Inc.* case. Asserting domestic data protection standards outside a jurisdiction's borders may clash with duties of international comity and the need to respect diversity of legal systems. In fact, the balance between the right to be forgotten, freedom of information and free speech is struck differently in jurisdictions around the world – including states that share the same belief in democracy, the rule of law and human rights. Moreover, as the recent judgments of the Canadian and US courts point out, the enforcement of data protection standards outside a jurisdiction's borders may ultimately be nullified by opposite claims. In the Canadian Google litigation, in particular, the US federal district court blocked the application of the Canadian Supreme Court ruling – de facto limiting the application of the Canadian writ in the US jurisdiction.

In light of these risks, the recent judgments of the ECJ in *Google v. CNIL* and *Glawischnig-Piesczek v. Facebook* can be seen as a pragmatic solution, trying to navigate between the Scylla of data protection imperialism and the Charybdis of digital sovereignty. In fact, it is clear that tensions between these opposing trends are only likely to increase. While criticism have been raised at the 'imperialist' attitude of EU data protection law,[81] other recent developments, including efforts by countries around the world to claim sovereign control over data, expose the risk of a fragmentation of the

[79] *Google v. CNIL* (n 52) at 72.

[80] See Article 29 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-131/12' (2014) WP225 at 9.

[81] See Dan Jerker B Svantesson, 'The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach' (2015) EUI Working Papers <http://cadmus.eui.eu//handle/1814/36317> accessed 15 January 2020; Ravi Shankar Prasad, 'India Views Its Privacy Seriously, Data Imperialism Not Acceptable' [2019] The Economic Times <https://economictimes.indiatimes.com/tech/ites/india-views-its-privacy-seriously-data-imperialism-not-acceptable-ravi-shankar-prasad/articleshow/71937835.cms?from=mdr>.

digital world. Different claims to digital sovereignty are emerging not only in the US[82] or the EU for that matter[83] – but also in illiberal regimes around the world,[84] potentially generating a progressive erosion of fundamental rights online. In this context, the development of transnational legal frameworks – at least among democratic regimes – seems to be the necessary path to preserve data protection rights beyond borders.

VII. Conclusion

The EU is at the forefront of data protection worldwide. The GDPR represents the most comprehensive and advanced regulatory framework for data privacy to date – and the ECJ has developed a progressive case law to protect human rights in the digital age, including outlining a right to be forgotten. In fact, the EU data protection law framework has proved so resilient that it has resisted even the outbreak of Covid-19, the largest pandemic the world experienced in a century: despite the effort to develop new digital technology to map and track contagions, data privacy concerns shaped the process, and ultimately avoided solutions which would have traded privacy in favor of health rights.

Nevertheless, despite its inherent strength, EU data protection law generally – and the right to be forgotten specifically – are increasingly facing a question of jurisdictional boundaries. From an EU perspective, the extraterritorial enforcement of EU fundamental rights is regarded as a way to guarantee a full and effective protection and prevent the risk of circumvention. However, the reach of EU data protection law beyond the EU borders also raises a series of challenges, clashing with the principles of international comity and respect for global diversity.

The issue of extraterritorial application of EU data protection law was at the heart of two recent judgments decided by the ECJ: in *Google v. CNIL* and *Glawischnig-Piesczek* v. *Facebook*, the ECJ dealt with the question of whether the right to be forgotten and the obligation to remove defamatory content applied worldwide or not. In the first case, the ECJ ruled that the removal was restricted to EU member states only, while in the second it allowed a world-wide injunction. In both cases, however, the ECJ showed awareness for the cross-borders implications of its decisions and for the need to recognize transnational diversity and international comity, thus finding pragmatic solutions to modulate the effects of EU data protection law beyond the EU borders.

As this chapter has shown, the challenges that the ECJ was facing are not unique to Europe. Other jurisdictions such as Australia and Canada were also confronted with the dilemma of how to protect digital rights across borders. Theoretically, contemporary digital society, being global, would require worldwide rules. However, the extraterritorial

[82] See Clarifying Lawful Overseas Use of Data (CLOUD) Act, PL 115-141. The statute was purposefully adopted as a response to a case in which Microsoft contested a search warrant aiming to gather data stored on its Irish servers: see Dan Svantesson and Felicity Gerry, 'Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond' (2015) 31 Computer Law & Security Review 478.

[83] See European Commission, 'European Cloud Initiative - Building a Competitive Data and Knowledge Economy in Europe' (2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0178&from=EN>.

[84] In 2017, China passed a new National Intelligence Law obliging companies to collaborate with Chinese intelligence agencies. The act de facto requires companies incorporated in China to disclose data that may have been collected and stored abroad to Chinese authorities: see See Yi-Zheng Lian (n 11). In the context of the trade war with the US, the legislation produced strong criticism, the US lamenting that a similar obligation could put in danger their national security.

application of data protection standards also raises significant challenges. In fact, the protection of privacy in the digital age increasingly exposes a tension between efforts by legal systems to impose their high standards of data protection outside their borders – and thus potentially regarded as a form of 'imperialism' –and sovereigntist claims by other legal systems to assert their own power over data.

In this context, states should seek to develop common international law frameworks, which promote transnational standards of data protection. Admittedly, this will not be an easy task. However, this is something that should be explored, particularly among liberal democracies, and at least in the transatlantic context.[85] Despite differences, jurisdictions such as the EU, Canada and Australia – as well as the US[86] – share a similar concern for the need to protect privacy, which puts them at odds with developments in other countries, such as China or Russia. Developing transnational rules for the protection of digital privacy, including outlining mutually acceptable claims to the right to be forgotten, represents therefore the best road forward to make sure that privacy remains a protected right, also in the digital era.

[85] See David Cole, Federico Fabbrini and Stephen J Schulhofer (eds), *Surveillance, Privacy, and Transatlantic Relations* (Hart Publishing 2017).
[86] See Fischer, Chapter 3.