Common Market Law Review **59**: 969–1006, 2022.

THE CONSTRUCTION OF A EUROPEAN DIGITAL CITIZENSHIP IN THE CASE LAW OF THE COURT OF JUSTICE OF THE EU

ANASTASIA ILIOPOULOU-PENOT*

Abstract

The case law of the Court of Justice on the prohibition of general (meta)data retention and on the right to be forgotten, has formed the cradle for a new status protecting and empowering the data subject. Built upon a distinctive equilibrium of values and linked to the territory of the Union, the new status can be described as an embryonic European digital citizenship. The article explores the construction of the new status orchestrated by the Court of Justice in close interplay with national courts (especially apex courts) and the EU legislature. It identifies various ways in which the case law of the ECJ on digital rights is similar to the case law on Union citizenship. The emerging status then opens up a new vista of how citizenship can be understood and developed in the EU legal order beyond the framework of Articles 20 and 21 TFEU, in order to address the challenges of an increasingly digitized society.

1. Introduction

On 9 March 2021, the European Commission presented its vision and strategy for Europe's digital transformation by 2030.[1] As part of its action within this framework, on 26 January 2022, the Commission proposed an inter-institutional solemn declaration of a set of digital principles and rights.[2] The adoption of such a declaration would be a welcome move, offering

* Professor of European Law, University Paris Panthéon-Assas, Centre for European Law.
I am indebted to Siofra Collins and Thomas Maddock for useful comments as well as to the anonymous reviewers for suggestions which contributed significantly to the final version of the article. The usual disclaimer applies.

1. See European Commission, "Europe's Digital Decade: digital targets for 2030", at <ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030> (all websites last visited 11 May 2022).

2. COM(2022)27 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Establishing a European Declaration on Digital rights and principles for the Digital Decade; COM (2022)28 final, "European Declaration on Digital Rights and Principles for the Digital Decade".

political impetus to the process of creating a "digital citizenship",[3] i.e. a new form of citizenship which guarantees "the ability to participate in society online".[4] In this respect, a significant legal development has already taken place in the case law of the ECJ on the protection of personal data, considerably reinforcing the legal position of the "data subject".[5] This case law has come into the spotlight, as it attests to the ability of EU law and the Court of Justice to address the challenges raised by the functioning of the information society and the use of big data. It is submitted in this article that this case law also signals the beginning of a transformative process occurring within the EU legal order: the internet user or "data subject" progressively becoming a European digital citizen. The case law edifice contributing to this transformation essentially rests on two pillars – the first relating to the retention of traffic and location data, and the second to the right to be forgotten – which are summarized below.

The first line of case law concerns the retention of traffic and location data, also known as (meta)data. In the groundbreaking judgment *Digital Rights Ireland*,[6] the ECJ struck down Directive 2006/24,[7] the adoption of which reflected the serious security concerns of Member States in the aftermath of several terrorist attacks in European cities (Madrid in 2004 and London in 2005). The Directive imposed on telecommunications providers the duty to retain traffic and location data in order to make them available to public authorities for law enforcement purposes (particularly combatting serious crime).[8] Emboldened by Articles 7 and 8 CFR, the Court established the principle of prohibition of mass preventive retention and instructed the EU legislature to provide for (meta)data retention which is targeted and

3. The Commission uses the term "digital citizenship" in its statement announcing its strategy for Europe's digital transformation, also called the 2030 Digital Compass, cited *supra* note 1.

4. This is the definition of digital citizenship given by Mossberger, Tolbert and McNeal, *Digital Citizenship. The Internet, Society and Participation* (MIT Press, 2007).

5. "Data subject" is the term used by the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, O.J. 2016, L 119/1.

6. Joined Cases C-293 & 594/12, *Digital Rights Ireland and Seitlinger and others*, EU:C:2014:238.

7. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. 2006, L 105/54.

8. It was the first time that an entire piece of secondary law was declared invalid by the ECJ for violation of the EU Charter of Fundamental Rights.

surrounded by robust safeguards. The subsequent judgment in *Tele 2*[9] set the same high standard of data privacy for the national legislature as that applied to the EU legislature under *Digital Rights Ireland*.[10] As a consequence, only national measures providing for targeted (meta)data retention and accompanied by strict safeguards are likely to comply with Directive 2002/58 (the Directive on ePrivacy),[11] read constructively in the light of the Charter. Despite some critical reactions, the ECJ upheld the principle of prohibition of general and indiscriminate retention of (meta)data, in the follow-up case *La Quadrature du Net*.[12] At the same time, essentially responding to the national governments arguing their need to combat terrorism, the Court introduced an exception for the sole purpose of safeguarding *national security* in the face of a serious, genuine and present (or foreseeable) threat. On the contrary, the purposes of combatting serious crime and safeguarding *public security* can only be invoked to justify measures of targeted retention.[13]

9. Joined Cases C-203 & 698/15, *Tele2 Sverige AB* v. *Post-ochtelestyrelsen and Secretary of State for the Home Department* v. *Tom Watson*, *Peter Brice and Geoffrey Lewis*, EU:C:2016:970.

10. Writing extrajudicially, the President of the ECJ highlights this parallelism. See Lenaerts, "The European Union as a Union of democracies, justice and rights", (2017) *International Comparative Jurisprudence,* available at <dx.doi.org/10.13165/j.icj.2017.12.001>: "the EU as a Union of rights also means that the fundamental rights recognized in the Charter offer the same level of protection regardless of whether limitations to those rights are adopted at national or EU level. The EU system of fundamental rights protection does not apply double standards. ... *Digital Rights* (2014) and *Tele2 Sverige and Watson* (2016) demonstrate that, when it comes to the right to privacy, both the EU and national legislators are subject to the same standards of protection."

11. Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. 2002, L 201/37.

12. Joined Cases C-511, 512 & 520/18, *La Quadrature du Net* v. *Premier ministre and others*, EU:C:2020:791; see also Case C-623/17, *Privacy International* v. *Secretary of State for the Home Department,* EU:C:2020:790.

13. The distinction between, on the one hand, national security and, on the other hand, public security and combatting serious crime, is essential for the ECJ. As it notes in Joined Cases C-511, 512 & 520/18, *La Quadrature du Net*, paras. 135 and 136: "Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilizing the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities. The importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combatting crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in the preceding paragraph can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down

The strand of case law on (meta)data retention[14] is completed and extended in *Schrems I and II*,[15] in relation to the Union's external action. The *Schrems* saga forcefully illustrates that EU standards for guaranteeing online privacy apply to the transfer of data outside the territory of the Union. Applying the strict *Digital Rights Ireland* doctrine, the ECJ struck down the Commission's adequacy decision on the EU-US Safe Harbour Framework[16] and, later, the Privacy Shield Framework,[17] both of which authorized data transfers to servers located in the US. According to the Court, these decisions did not comply with the requirements of Directive 95/46[18] (in *Schrems I*) and the General Data Protection Regulation[19] (in *Schrems II*), read in the light of Articles 7 and 8 CFR,[20] because of the excessively intrusive surveillance programmes in place in the US. The Court strategically chose to interpret "adequate" data protection required for outward transfers as "essentially equivalent" to that afforded by EU law, thereby considerably elevating the standard of protection and reducing the European Commission's negotiating discretion.

The second line of case law, consisting of several cases involving Google, concerns the right to be delisted (referred to also as de-referencing, but more commonly referred to as the right to be forgotten). The judicial recognition of

in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives."

14. Case C-207/16, *Ministerio Fiscal,* EU:C:2018:788*,* and Case C-746/18*, Prokuratuur (Conditions of access to data relating to electronic communications),* EU:C:2018:788*,* complete this strand of case law, while adding some points of detail.

15. Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner*, EU:C:2015: 650 (*Schrems I*); Case C-311/18, *Data Protection Commissioner* v. *Facebook Ireland Ltd, Maximillian Schrems*, EU:C:2020:559 (*Schrems II*).

16. Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, O.J. 2000, L 215/7.

17. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, O.J. 2016, L 207/1.

18. Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. 1995, L 281/31.

19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016, L 119/1.

20. The ECJ also found a breach of the right to an effective remedy, enshrined in Art. 47 CFR, because data subjects do not have actionable judicial redress under the US regime.

this right in *Google Spain*,[21] a judgment handed down shortly after *Digital Rights Ireland* and again anchored in Articles 7 and 8 CFR, confirms the ECJ's willingness to be the vanguard in the protection of personal data. Indeed, the Court spells out the right of data subjects to have their data removed from the list of results provided by online search engines, even if the content was lawfully displayed, and without having to demonstrate prejudice. Then, in its subsequent judgment in *Google LLC*,[22] the Court determined the *territorial* scope of the right to be delisted, specifying that it concerned only the national versions of a search engine corresponding to all the Member States.[23] It also defined, in *G.C.*,[24] the *material* scope of the right, which also includes data considered to be "sensitive" (i.e. revealing racial or ethnic origin, political opinions or religious or philosophical beliefs, or concerning the health or sex life of an individual) as well as data related to criminal convictions and offences.

The ECJ's case law on the protection of personal data has been closely followed and extensively analysed, also outside legal circles. This is logically explained by the considerable practical consequences it entails for private operators, for national regulators, and for EU institutions, both in the legislative process and in the field of external relations. This salient case law has rightly been seen as concretizing the normative potential of the Charter of Fundamental Rights, with the ECJ donning "with confidence the clothes of a human rights court"[25] and overtaking national (constitutional and supreme) courts in guaranteeing digital rights. This case law has also been approached from the perspective of data or digital sovereignty, which is a growing component of the political and legal discourse on European sovereignty.[26] Thus, the Court's recognition of "the existence of an *imperium* of European dimension over personal data"[27] has been welcomed by some authors as

21. Case C-131/12, *Google Spain* v. *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, EU:C:2014:317.

22. Case C-507/17, *Google LLC* v. *CNIL*, EU:C:2019:772.

23. On the extra-territoriality aspects of the case, see Fabbrini and Celeste, "The right to be forgotten in the digital age: The challenges of data protection beyond borders", 21 GLJ (2020), 55.

24. Case C-136/17, *G.C. and others* v. *CNIL*, EU:C:2019:773.

25. Fabbrini, "The EU Charter of Fundamental Rights and the rights to data privacy: The EU Court of Justice as a human rights court", iCourts Working Paper Series, No. 19, 2015.

26. Bertrand, "La souveraineté numérique européenne: une 'pensée en acte'?", (2021) RTDE 2021, 249; G'Sell, "Remarques sur les aspects juridiques de la 'souveraineté numérique'", (2020) Revue ScPo, 52; Celeste, "Digital sovereignty in the EU: Challenges and future perspectives" in Fabbrini, Celeste and Quinn (Eds.), *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart, 2021), p. 211.

27. Benabou, "La Cour de justice, gardienne d'une 'souveraineté européenne' sur les données personnelles", (2018) R.A.E., 20.

guaranteeing the rights of individuals.[28] Others have been more sceptical, reading the Court's case law as an attempt to build a "European personal data fortress" and as an excessive Europeanization of the regulation of the internet, the transnational character of which is incompatible with the logic of regional protection.[29]

There is, however, an essential dimension to this landmark case law, which has not, as yet, been sufficiently highlighted in legal literature. In fact, the ECJ is steadily building, "stone by stone",[30] a coherent set of rights and guarantees for the individual acting in the cyberspace. In other words, we are witnessing the emergence of a special *status* focused on the protection of "data privacy", defined by Fabbrini as "a number of entitlements that individuals shall enjoy when interacting in the digital world".[31] We submit that this nascent status can be described as an embryonic European digital citizenship[32] as it presents (even if it is not yet in a fully-fledged manner) several features which are commonly found in accounts of citizenship.[33] As the article shows, first, the new status aims at the protection of the individual both against the exercise of power by traditional public authorities, now equipped with new technological means, and against unprecedented forms of power of private corporations dominating the digital realm. In this way, the new status guarantees individual autonomy and the ability to interact meaningfully with others in the public space redefined by internet. Second, the emerging status is built upon a distinctive equilibrium of values, which prioritizes data privacy over conflicting fundamental rights and weighty interests, and which makes the US Europe's "Other". Digital rights then become a stepping stone for expressing, fostering and asserting a European collective identity, embedded in the Charter; this evolution confirms the identity-building capacity of the Union's

28. Ibid.; Lynskey, "The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*", 51 CML Rev. (2014), 1789.

29. See Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?* (Hart, 2021), especially Ch. 3 "Judges, privacy and data protection: From atoms to bits across the Atlantic", pp. 99 et seq.

30. On the "stone-by-stone approach" see Lenaerts, "The Court's outer and inner selves: Exploring the external and internal legitimacy of the European Court of Justice" in Adams, de Waele, Meeusen and Straetmans (Eds.), *Judging Europe's Judges* (Hart, 2013), p. 13.

31. Fabbrini, op. cit. *supra* note 25.

32. For an early reference to the term "digital citizenship" in order to describe what is taking place in the ECJ's case law on data protection, see Simon, "La révolution numérique du juge de l'Union: Les premiers pas de la cybercitoyenneté", (2014) *Europe*, Étude 5.

33. See Shachar, Bauböck, Bloemraad and Vink (Eds.), *The Oxford Handbook of Citizenship* (OUP, 2017) especially the "Introduction: Citizenship – *Quo Vadis?*" by the three editors.

Bill of Rights.[34] Third, as the personal data of the individual present in the EU can only be transferred to third countries offering essentially equivalent data protection standards, the emerging status is linked to the *territory of the Union*, which refers to "a special legal place and a special common place", "with strongly protective implications for Union citizens".[35] European digital citizenship can then be described as a protective personal status which gives concrete expression to membership in the EU, as a polity committed to upholding distinctive values and rights in society, also in its online dimension. This vision underpins the case law of the ECJ, chief architect of the legal construction of the new status. Its judgments in the field of personal data have been game-changers as they have informed the litigation strategies of individuals and civil society organizations defending digital rights. They have also sparked action by other EU institutions, by national courts (especially apex courts), by national data protection authorities, and by the European Data Protection Supervisor. This action contributes to further nurturing the process set in motion by the Court's case law creating a new form of citizenship rising to the challenges of the information society.

This qualification of the new status based on data privacy as European digital citizenship begs the question of its relationship to Union citizenship, established under Article 20 TFEU. It is submitted that the new status is distinct and yet related to Union citizenship. Indeed, European digital citizenship is not rooted in the same primary law provisions and is not concretized by the same secondary law instruments as Union citizenship. It has its own legal framework, formed by Articles 7 and 8 CFR, Article 16 TFEU and the GDPR. Furthermore, neither the Court nor the EU legislature use the concepts of "citizenship" or "fundamental status"[36] to describe the set of rights associated with data privacy. Still, the process of its elaboration has a familiar ring to it, it evokes a feeling of *déjà vu*. In fact, it relies on the same actors and shares the methods and tools used in the construction of the status of Union citizen, which has been in progress for a number of years.[37] Indeed,

34. See Iliopoulou-Penot and Xenou, "Propos introductifs. De la capacité de la Charte de façonner une identité de l'Union dans un contexte pluraliste" in Iliopoulou-Penot and Xenou (Eds.), *La Charte des droits fondamentaux, source de renouveau constitutionnel européen?* (Bruylant, 2020), p. 17.

35. Nic Shuibhne, "The 'territory of the Union' in EU Citizenship law: Charting a route from parallel to integrated narratives", 38 YEL (2019), 267, respectively at 305 and at 313. This point is returned to later in detail.

36. Introduced in para 31 of the judgment in Case C-184/99, *Rudy Grzelczyk* v. *Centre Public d'aide d'Ottignies-Louvain-la Neuve*, EU:C:2011:458; this formula has constituted a *leitmotiv* of the case law on Union citizenship.

37. Especially since the groundbreaking judgments in Case C-85/96, *Maria Martínez Sala* v. *Freistaat Bayern*, EU:C:1998:217; Case C-413/99, *Baumbast and R* v. *Secretary of State for the Home Department*, EU:C:2002:493; Case C-184/99, *Grzelczyk*. A remarkable account of

in both cases, the Court of Justice has assumed a pioneer role through its groundbreaking teleological interpretation of primary law. It has put flesh on the bones of the Treaty provisions on Union citizenship[38] guided by its *telos* as a "fundamental status", vesting the individual with protection and enabling them to uphold certain life choices. Similarly, the Court has breathed life into the Charter provisions concerning respect for privacy and personal data, using these fundamental rights as the cornerstones of the new status for the European internet user enhancing their autonomy and capacity of control over their data. The two bodies of law (on Union citizenship, established under Art. 20 TFEU and on European digital citizenship) are then underpinned by a particular philosophy, by a certain vision of the European individual, as a subject empowered and protected by the EU legal order, and of Europe as a distinctive geographical, legal and normative space.

There is thus sufficient proximity to sustain the view that both legal developments (on Union citizenship and on digital rights) can be properly characterized as being part of the same family. Union citizenship, established by Article 20 TFEU, can be regarded as standing at the core of a broader "European citizen paradigm", which may embrace other bodies of EU law,[39] such as the evolving set of digital rights. This set of rights grows in parallel with, and draws implicit inspiration from, the status of Union citizenship, while also applying to third-country nationals present on the territory of the Union. The emerging status then opens up a different vista of how citizenship can be understood and developed in the EU legal order beyond the framework of Articles 20 and 21 TFEU, in order to address the challenges of an increasingly digitized society. It can therefore contribute to maintaining a dynamic and open-textured concept of European citizenship.

The article narrates the story of the nascent European digital citizenship, focusing on its commonalities with Union citizenship. It explores the construction of a new status orchestrated by the Court of Justice[40] (section 2) in close interplay with other actors on the European stage, in particular

the evolution is provided (in French) by Carlier, "La citoyenneté européenne: de la coque aux cerneaux" in Paschalidis and Wildermeersch (Eds.), *L'Europe au présent! Liber amicorum Melchior Wathelet* (Bruylant, 2018), p. 287, and (in English) by Coutts, "The shifting geometry of Union citizenship: A supranational status from transnational tights", 21 CYELS (2019), 318.

38. The expression is borrowed from O'Leary, "Putting flesh on the bones of European Union citizenship", 24 EL Rev. (1999), 68.

39. EU anti-discrimination law can also be regarded as being part of the broader "European citizenship paradigm" as it shares concepts, methods and objectives with the pillar on Union citizenship. It also embodies a particular conception of the place of the individual within society.

40. For an early account of the Court's role in the construction of Union citizenship see Kostakopoulou, "Ideas, norms and European citizenship: Explaining institutional change", 68 *Modern Law Review* (2005), 233.

national courts and the EU legislature (section 3). It seeks to analyse the way in which the institutional dynamics at play and the trajectory followed for the building of the new regime have influenced its substance. In particular, the article identifies various ways in which the case law of the ECJ on digital rights is similar to the case law on Union citizenship. Comparison with the latter helps us better understand how the former is currently evolving and allows us to reflect on the direction it is likely to follow. The conclusions drawn are summarized in section 4.

2. A new judge-made citizenship

The building of European digital citizenship by the ECJ essentially involves granting rights and guarantees to data subjects. In other words, it is driven by the classic rights-based approach (section 2.1). While this is where the strength of the process lies, it is also the main source of criticism levelled at it (section 2.2).

2.1. *The rights-based approach, again*

European digital citizenship is built bottom-up, through the assertion of rights, generating claims. Battles for rights often have a face and the battle to defend e-privacy in Europe is probably best represented by the activist Max Schrems, who is at the origin of the ECJ's judgments that proudly bear his name.[41] He is not alone in this fight. His concerns are shared by a growing number of Europeans, who have become aware of the issues at stake following Edward Snowden's revelations of large-scale intelligence collection programmes in the US.[42] This is evidenced by the fact that 11,000 citizens joined the proceedings brought by the Austrian *Land* of Carinthia before the *Verfassungsgerichtshof*, culminating in the *Digital Rights Ireland* judgment of the ECJ. Furthermore, the vigilance and mobilization of civil society has been a decisive factor in assuring data protection. Legal action initiated by

41. The litigation that led to the ECJ's judgments in *Schrems I and II* is part of the wider action of the group *My privacy is none of your business*, see <noyb.eu>, founded by Max Schrems.

42. The importance of not being alone in the fight for the protection of e-privacy is recognized in Edward Snowden's tweet after the *Big Broth*er judgment, ECtHR, *Big Brother Watch and others* v. *UK*, Appl. Nos. 58170/13, 62322/14 & 24960/15, judgment of 25 May 2021: "Without journalists to tell the story, the public would not have known about it. Without human right lawyers defending that public, the courts would not have cared about it. Without those courts, politicians would still be denying it. I could not have done this alone."

organizations campaigning for e-privacy[43] involves a litigation strategy aimed at reaching the European courts, either by seeking the annulment of a European measure or by requesting a preliminary reference. Thus, the NGO Digital Rights Ireland, at the origin of the ECJ's preliminary judgment carrying its name, also sought the annulment of the Commission's adequacy decision on the EU-US Privacy Shield Framework before the General Court.[44] The same decision was challenged by the advocacy groups La Quadrature du Net and French Data Network,[45] which are also protagonists in the long saga of litigation leading to the ECJ's judgment in *La Quadrature du Net* and to its questionable application by the French *Conseil d'Etat* in its *French Data Network* judgment.[46]

Individuals and advocacy groups leading the battle for the defence of e-privacy were right to turn to the ECJ. The Court has developed European digital citizenship as "the right to have rights"[47] when acting and interacting in the digital ecosystem. It strategically chose to frame all relevant cases as "issues of individual protection in a digital world dominated by public or private corporate players".[48] Using the rights-based approach, which has already been tested with success in the case law laying the foundations for Union citizenship, the Court is currently building a protective status for the European digital network user. The Court has thus spelled out, as a component of this status, a right to have "information removed from the 'active memory' of the Internet".[49] This right meets a genuine societal need, a fact which is attested by the large number of requests made to Google to remove online content.[50] The Court has also equipped individuals with the right to defend

43. Such action is bound to be expanded after the ECJ's judgment in Case C-319/20, *Meta Platforms Ireland*, EU:C:2022:322. Following the Opinion of A.G. Richard de la Tour, the Court considers that the GDPR does not preclude national legislation which allows consumer protection associations to bring representative actions against infringements of the laws protecting personal data. The associations do not need to have a mandate from the data subjects nor claim the existence of actual cases affecting named individuals.

44. Case T-670/16, *Digital Rights Ireland Ltd* v. *European Commission*, EU:T:2017:838.

45. Case T-738/16, *La Quadrature du Net and others* v. *European Commission*, EU:T:2020:638.

46. CE, Ass., 21 avril 2021, *French Data Network e.a.,* Nos. 393099, 394922, 397844, 397851, 424717, 424718.

47. Following the classic formula of Arendt, *The Origins of Totalitarianism* (Schoken Books, 2004), p. 293.

48. See Azoulai and Van der Sluis, "Institutionalizing personal data protection in times of global institutional distrust: *Schrems*", 53 CML Rev. (2016), 1343.

49. Buchta and Kranenborg, "General Report topic 2: The new EU data protection regime" in Rijpma (Ed.), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection* (FIDE, 2020, Vol. 2), p. 79.

50. Tambou, "Protection des données personnelles: les difficultés de la mise en œuvre du droit européen au déréférencement", (2016) RTDE, 249.

themselves against practices of systematic electronic surveillance.[51] Indeed, such practices entail serious risks for privacy, as the use of collected metadata can reveal individuals' habits, social interactions and personal preferences, even intimate ones. The ECJ expressly recognizes this capacity of detailed profiling and its adverse effects on individuals. It thereby underlines that (meta)data can be used to establish "a profile of the individuals concerned";[52]

> "taken as a whole, [such data] may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[53]

The rights recognized by the ECJ aim at enhancing individual autonomy and at preserving the ability to exercise control over one's own personal data. The two key words of the European discourse on data protection, namely autonomy and control,[54] underpin the Court's reasoning. The case law promotes the empowerment of the individual *vis-à-vis* national governments and *vis-à-vis* mighty private corporations. Such empowering logic has its roots in the case law on Union citizenship, which developed as a status protecting the activities and integration of European individuals beyond national borders.[55] The case law on European digital citizenship transposes and extends this logic by vesting the individual acting in the digital realm with a panoply of protections. Significantly, this panoply is also characterized by a

51. Ojanen, "Privacy is more than just a seven-letter word: The Court of Justice of the European Union sets constitutional limits on mass surveillance", 10 EuConst (2014), 528; Ojanen, "Rights-based review of electronic surveillance after *Digital Rights Ireland* and *Schrems* in the European Union" in Fabbrini and Schulhofer (Eds.), *Surveillance, Privacy and Transatlantic Relations* (Hart, 2017), p. 13.

52. Joined Cases C-203 & 698/15, *Tele2*, para 99; Joined Cases C-511, 512 & 520/18, *La Quadrature du Net*, para 117.

53. Joined Cases C-293 & 594/12*, Digital Rights Ireland*, para 27; Joined Cases C-203 & 698/15, *Tele2*, para 99*;* Joined Cases C-511, 512 & 520/18, *La Quadrature du Net*, para 117.

54. European Commission, *It's Your Data – Take Control*: "The EU's data protection rules give you more control over your personal data . . . Check out your rights, take control.", available at <ec.europa.eu/info/sites/default/files/data-protection-overview-citizens_en_0.pdf>.

55. Azoulai, "La citoyenneté européenne, un statut d'intégration sociale" in *Chemins d'Europe. Mélanges en l'honneur de Jean-Paul Jacqué* (Dalloz, 2010), p. 1; Iliopoulou-Penot, "The transnational character of Union citizenship" in Dougan, Spaventa and Nic Shuibhne (Eds.), *Empowerment and Disempowerment of the European Citizen* (Hart, 2012), p. 15.

"principle of continuity",[56] which ensures that the protection provided is not circumvented by data transfers to third States. The ECJ's case law on data protection can thus be seen as responding to the widespread perception within European societies that individual command has been lost in the digital realm; it illustrates the will to "take back control".

Without a doubt, the case law on European digital citizenship is a typical example of judicial activism. Such activism was initially facilitated by the fact that the applicable legislative framework (i.e. Directives 95/46 and 2002/58) had been overtaken by evolution in the digital sphere. Invoking the Charter allowed for a dynamic and updated interpretation of secondary law. The constitutionalization of the right to protection of personal data by its inclusion in Article 8 CFR,[57] following respect for private life enshrined in Article 7, legitimized the ECJ's effort to establish guarantees for the network user. In a similar way, in the past, the establishment of Union citizenship had encouraged the advent of a case law movement safeguarding the rights of mobile Europeans. The plasticity of the interpreted provisions (Arts. 7 and 8 CFR) has been creatively exploited by the ECJ. The adoption of the GDPR has supported the Court's approach, since this new legislative instrument has clearly been formulated in the spirit and language of the "fundamentality" of the right to protection of personal data, as indicated in its Recitals 1 and 11.[58]

Moreover, the case law on data protection is a further illustration of the Court's technique, which is already tried and tested in the case law on Union citizenship. This technique consists in turning one individual's problem into a matter of principle and constitutional importance, in transforming a small personal issue into a wider political agenda. Thus, just as the refusal of the *minimex* to a French student in Belgium was the catalyst for European social citizenship,[59] M. Gonzalez Costeja's embarrassment in being constantly confronted by his past debts and the seizure of his real estate, gave rise to the

56. See Cruz Villalon, "Un principe de continuité? Sur l'effet extraterritorial de la Charte des droits fondamentaux de l'Union européenne" in Paschalidis and Wildermeersch op. cit. *supra* note 37, p. 317.

57. See Kranenborg, "Article 8 – Protection of personal data" in Peers, Hervey, Kenner and Ward (Eds.), *The EU Charter of Fundamental Rights. A Commentary* (Hart, 2021), p. 223.

58. Under the first Recital, "the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her." Under Recital 11, "effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States."

59. Case C-184/99, *Grzelczyk*.

recognition of the need to remove online content in the EU legal corpus of data protection. In the same way that the student Rudy Grzelczyk became the emblematic jurisprudential figure of belonging to a transnational community of solidarity, M. Gonzalez Costeja is seen by the Court as "a member of the EU community, in that he is not only entitled to its protection against the digital giants but also that he is placed within a certain social ordering by being characterized as a private figure whose data should therefore not be of interest to the wider public".[60]

Furthermore, the ECJ does not hesitate to strike "its own balance of values"[61] in the case law on data protection, which perforce implies choices of a political nature. The Court settles delicate conflicts between respect for data privacy, on the one hand, and security (in the cases related to metadata retention) or freedom of expression and information (in the cases on the right to be forgotten), on the other. These complex balancing operations[62] allow the shaping of the contours of European digital citizenship. Indeed, every form of citizenship rests on an equilibrium of values, that is patiently designed (and adjusted) and expresses a particular conception of the individual and their place within the community. The ECJ has already engaged in this type of dialectical exercise in the case law on Union citizenship. It has had to rule on the conflict between the right of residence (especially long-term) and the imperatives of public policy and security (in the cases concerning the expulsion of Union citizens[63]). It has had to reconcile the requirements of equality and solidarity among European citizens, with the need to preserve the public finances of the States (in the cases concerning access of Union citizens to social benefits[64]). The case law in this field is characterized by a constant search of the "right" balance between the various legitimate concerns at stake.

It is at this point that a difference between the case law on Union citizenship and that on European digital citizenship can be observed. The former is composed of cycles, within which the conciliation of divergent interests

60. Marzal, "From world actor to local community: Territoriality and the scope of application of EU Law" in Azoulai (Ed.), *European Union law and Forms of Life: Madness or Malaise* (Hart, forthcoming).

61. Jacqué, "Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la CJUE", (2014) RTDE, 285.

62. A.G. Jääskinen emphasized "the particularly complex and difficult constellation of fundamental rights that this case presents" (Opinion in Case C-131/12, *Google Spain,* EU:C:2013:424, para 133), which led him to reject the recognition of the right to be delisted.

63. See e.g. Case C-145/09, *Land Baden Würtemberg* v. *Panagiotis Tsakouridis*, EU:C:2010:708; Case C-348/09, *P.I.* v. *Oberbürgermeisterin der Stadt Remscheid*, EU:C:2012:300.

64. See e.g. Case C-184/99, *Grzelczyk*; Case C-333/13, *Elisabeta Dano and Florin Dano* v. *Jobcenter Leipzig*, EU:C:2014:2358.

changes.[65] The "constituent" and "consolidation" phases that favoured individual rights were followed by a "reactionary" phase, demonstrating a heightened sensitivity to State interests.[66] A new cycle seems to be evolving currently, characterized by a more balanced (albeit not always convincing) approach to individual rights and State interests.[67] On the contrary, the case law on European digital citizenship is – at least for the time being – remarkably constant.[68] It embodies a highly demanding European conception of data privacy, perceived as a leading right which overshadows competing rights and other weighty interests. Thus, the prohibition of generalized data retention is formulated as a rule and its authorization as a derogation. Indeed, according to the European jurisprudential credo, "it is necessary, within a democratic society, that retention be the exception and not the rule".[69] Similarly, delisting requested by the individual is presented as obligatory for the operator of a search engine as *a matter of principle*, whereas its refusal is seen as an exception. Indeed, the Court considers that the right to be forgotten must "in principle" prevail over the public's right to information; it can only be sidestepped if there is a "*preponderant* interest" of the general public to have access to the disputed information.[70] In other words, there is a strong presumption in favour of e-privacy, which is difficult to rebut.

It will be interesting to see whether the ECJ will be open to reconsidering the priority it has given to the protection of e-privacy, just as it altered its earlier generous reading of the social rights of economically inactive citizens

65. See Nic Shuibhne, "Limits rising, duties ascending: The changing legal shape of Union citizenship", 52 CML Rev. (2015), 889.

66. Concerning these phases, see Spaventa, "Earned citizenship – Understanding Union citizenship through its scope" in Kochenov (Ed.), *EU Citizenship and Federalism: The Role of Rights* (Cambridge University Press, 2017), p. 204.

67. Case C-93/18, *Ermira Bajratari* v. *Secretary of State for the Home Department*, EU:C:2019:809; Case C-181/19, *Jobcenter Krefeld – Widerspruchsstelle* v. *JD*, EU:C:2020:794; Case C-709/20, *CG* v. *The Department for Communities in Northern Ireland*, EU:C:2021:602. On this judgment see O'Brien, "The great EU citizenship illusion exposed: Equal treatment rights evaporate for the vulnerable", 46 EL Rev. (2021), 801.

68. This is illustrated by the Court's sticking to its principled stance in Case C-140/20, *GD* v. *Commissioner of the Garda Síochána,* EU:C:2022:258.

69. Joined Cases C-511, 512 & 520/18, *La Quadrature du Net*, para 142. In para 84 of the subsequent judgment in Case C-140/20, *GD*, the Court emphasizes that "the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general retention of traffic and localization data".

70. Case C-131/12, *Google Spain*, para 97 (emphasis added). Such "preponderant interest" has to be justified by "particular reasons, such as the role played by the data subject in public life".

in the host State.[71] This change occurred following criticism by certain governments and in some of the academic commentary concerning the initial position of the Court. Similar criticism currently targets the Court's case law on digital rights.

2.2. *Criticism: Has the Court gone too far?*

The case law edifice on European digital citizenship has been the subject of twofold critique, which is strongly reminiscent, in its essence, of the criticism triggered by the case law that breathed life into Union citizenship.[72] It is useful to recall the two main grounds of this criticism: first, the ECJ was seen as "rewriting" EU legislation in the light of Union citizenship and the principles of equality and proportionality; second, the Court has redefined access of mobile Union citizens to the social system of Member States, while the Union has no competence in the field of redistribution. This twofold critique, emphasizing the "subversive" reading of secondary law in the light of primary law and the intrusion into a field of national competence, is reiterated with regard to the case law fleshing out European digital citizenship. Once again, it is considered by some that the ECJ has gone too far.[73]

These reactions are worth considering. They concern both the method of reasoning applied by the ECJ in data protection cases and the results obtained. It must be admitted that the case law sets out duties which are not imposed by the black letter of secondary law, but by a creative reading supported by the open-textured provisions of primary law (the Charter) and the principle of proportionality. Indeed, it is impossible to consider by a mere reading of their text that Directive 95/46 imposes an obligation to delist online content on the operator of a search engine[74] and that it requires from third States a level of

71. This shift has led, according to F. de Witte, to the emergence of a new type of subject: the liminal European. See de Witte, "The liminal European: Subject to the EU legal order", 40 YEL (2021), 56.

72. For one of the strongest expressions of such criticism, see Hailbronner, "Union Citizenship and access to social benefits", 42 CML Rev. (2005), 1245. For a more nuanced discussion, see Dougan, "The bubble that burst: Exploring the legitimacy of the case law on the free movement of Union citizens" in Adams, de Waele, Meeusen and Straetmans, op. cit. *supra* note 30, p. 127, and Thym, "Towards 'real' citizenship? The judicial construction of Union citizenship and its limits", ibid., p. 155.

73. See Sirinelli, "La protection des données de connexion par la Cour de justice: Cartographie d'une jurisprudence européenne inédite", (2021) RTDE, 313.

74. As A.G. Szpunar subsequently admits in para 44 of his Opinion in Case C-136/17, *G.C.*, EU:C:2019:14, the provisions of Directive 95/46 "do not lend themselves to an intuitive and purely literal application to such search engines."

protection *essentially equivalent* to EU standards in order for transfers of personal data to take place; finally, that Directive 2002/58 precludes national regimes which provide for general (meta)data retention. Only expansive readings guided by a particular conception of the protection of the individual in the cyberspace can lead to such outcomes, which raise further questions.

For example, is it not excessive to require delisting even when there is no evidence of prejudice caused to the data subject? Has the ECJ failed to understand Google's contribution to the emergence of a "public" capable of forming the "public opinion" that is essential for democratic self-governance?[75] Has it taken sufficient account of the consequences of its solution for the freedom of expression and information as well as for the freedom to conduct business, which are also guaranteed by the Charter (respectively by Arts. 11 and 16)? German Federal Courts are more sensitive to such rights when it comes to carrying out the balancing exercise. This is the case of the *Bundesverfassungsgericht*[76] as well as the *Bundesgerichtshof*. The latter calls the attention of the ECJ to the issue of the weighing of rights in its referral decision in the pending case C-460/20, concerning the obligation for de-referencing by the operator of a search engine in a case when the veracity of the content displayed is disputed by the parties. The German court notes that the conflicting rights and interests arising from Articles 7 and 8 CFR, on the one hand, and from Articles 11 and 16, on the other hand, "must be weighed up equally against one another".[77] In his Opinion, Advocate General Pitruzzella takes this concern seriously, noting that:

> "balance is to be struck between fundamental rights *of equal importance*, which constitute the prerequisites for the proper functioning of a democratic society. Therefore, it is not possible to argue that any one overrides another in abstract terms, rather it is necessary to strike a balance

75. This is the criticism strongly voiced by Post, "Data privacy and dignitary privacy: *Google Spain,* the right to be forgotten, and the construction of the public sphere", 67 *Duke Law Journal* (2018), 981: "the CJEU misunderstands the relationship between Google and the construction of the contemporary public sphere. *Google Spain* dismisses Google as a mere profit-making, data-processing corporation. But that interpretation of Google fails to appreciate how Internet search engines underwrite the virtual communicative space in which democratic public opinion is now partially formed. Google should have been accorded the same legal status as print media." The author supports this assertion by showing how newspapers created the modern democratic public sphere in an analogous way in the US in the 19th and 20th centuries.

76. Judgments of 6 Nov. 2019, 1 BvR 16/13, "Right to be forgotten I" and 1 BvR 276/17, "Right to be forgotten II". See Friedl, "A new European fundamental rights court: The German Constitutional Court on the right to be forgotten", *European papers*, European Forum, 24 March 2020.

77. Referral decision in pending Case C-460/20, *TU, RE* v. *Google LLC*, para 15.

> in such a way as to bring about a co-existence which causes the least possible infringement of each of the fundamental rights concerned".[78]

When it comes to (meta)data retention, is it appropriate to deprive States of an efficient instrument for combatting serious crime?[79] The ECJ is criticized for interfering in an unjustified manner in the way in which States exercise their sovereign powers and carry out their essential mission of maintaining security on their territories, expressly acknowledged by Article 4(2) TEU. Thus, in the wake of the judgment in *Tele 2*, a significant number of national governments have called for a renegotiation of the balance between freedom and security in the field of data retention. Their demand was largely endorsed by three national courts in their referral decisions for preliminary rulings: the French *Conseil d'Etat*, the Belgian Constitutional Court, and the Investigatory Powers Tribunal of London. As the French Government was not satisfied with the ECJ's position in *La Quadrature du Net*, it asked the *Conseil d'Etat* to declare the judgment *ultra vires* and, as a consequence, not to apply it. This regrettable and worrying request was a first in the history of French litigation. While the *Conseil d'Etat* categorically refused this course of action, it clearly asserted in its judgment in *French Data Network* that it was not convinced by the ECJ's answer.[80]

In addition to the above-mentioned criticisms, it may also be tempting to object that while the ECJ's approach may endow individuals with more entitlements, it is not capable of fleshing out a form of citizenship as such. It may be plausible, however, to speak of the building of a true citizenship, as the

78. Opinion in Case C-460/20, *TU, RE* v. *Google LLC,* EU:C:2022:271, para 17 (emphasis in original). In accordance with this logic, the A.G. suggests "a procedure for exercising the right to de-referencing, which places specific burdens on all the parties involved" (para 49). More precisely, "it is incumbent on the data subject to provide *prima facie* evidence of the false nature of the content the de-referencing of which is sought, where that is not manifestly impossible or excessively difficult, in particular with regard to the nature of the information concerned. It is for the operator of the search engine to carry out the checks which fall within its specific capacities, contacting, where possible, the publisher of the referenced web page. Where the circumstances of the case so indicate in order to avoid irreparable harm to the data subject, the operator of the search engine will be able temporarily to suspend referencing, or to indicate, in the search results, that the truth of some of the information in the content to which the link in question relates is contested." (para 50).

79. See Cameron, "A Court of Justice balancing data protection and law enforcement needs: *Tele2 Sverige* and *Watson*", 54 CML Rev. (2017), 1467; Hijmans, "Data protection and surveillance: The perspective of EU law" in Mitsilegas and Vavoula (Eds.), *Surveillance and Privacy in the Digital Era* (Hart, 2021), p. 235. According to this author, "*Tele 2* provoked serious criticism because it could prejudice effective law enforcement by removing historical communications data. It could even be argued that, in the absence of access to such historical data, states would be deprived of a possibility to carry out their mission to protect."

80. See the analysis *infra,* section 3.1.

dynamic currently at work in the case law is also about affirming "the existence of a certain form of collective identity".[81] The judgment in *Digital Rights Ireland* offers two important clues in this respect. On the one hand, the ECJ underlines the wide-ranging "interference with the fundamental rights *of practically the entire European population*".[82] On the other hand, the Court, referring to the Opinion of the Advocate General, who evokes the "vague feeling of surveillance",[83] places increased emphasis on the "feeling", likely to be generated in the minds of the persons concerned, "that their private lives are the subject of constant surveillance".[84] This intriguing reference to the "feeling" of surveillance probably originates from the decisions of the Constitutional Courts of Germany, Romania and the Czech Republic on the implementation of the Data Retention Directive.[85] Like its national counterparts, the ECJ shows awareness for a feeling which can be both diffuse and collectively shared.[86] In a similar manner, the recognition of the right to be forgotten can also be seen as a way of defending "practically the entire European population" from the "feeling" of being overwhelmed by the new form of power exercised by digital giants, such as the operators of search engines.

Moreover, concerning (meta)data retention, it should be added that unconstrained surveillance systems place pressure on the autonomy not only of individuals, but also of the European community as a whole. Respect for e-privacy is not only linked to the realization of personal freedom; it also has an impact on public life and, thus, a collective value.[87] To give but one example, Advocate General Cruz Villalón rightly recalls that generalized surveillance is "capable of having a decisive influence on the exercise by

81. Dubout, "Qui est le sujet des droits de la Charte? De l'être universel à l'être relationnel" in Iliopoulou-Penot and Xenou (Eds.), *La Charte des droits fondamentaux, source de renouveau constitutionnel européen?* (Bruylant, 2020), p. 279.

82. Joined Cases C-293 & 594/12, *Digital Rights Ireland*, para 56 (emphasis added).

83. Opinion of A.G. Cruz Villalon in Joined Cases C-293 & 594/12, *Digital Rights Ireland*, EU:C:2013:845, paras. 52 et 72.

84. Joined Cases C-293 & 594/12, *Digital Rights Ireland*, para 37.

85. Benedizione and 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", 20 GLJ (2019), 1727.

86. Editorial comments, "EU law between common values and collective feelings", 55 CML Rev. (2018), 1329.

87. Seubert and Becker, "The democratic impact of strengthening European fundamental rights in the digital age: The example of privacy protection", 22 GLJ (2021), 31, at 32: "By strengthening people's personal freedom, European privacy protection is, at the same time, proving to be essential for the development and flourishing of democratic practices conceptualised as collective acts of free communication."

European citizens of their freedom of expression and information",[88] which is a cornerstone of democratic society. This example confirms that it is important to move beyond the individualistic prism and adopt a social understanding of respect for e-privacy as a collective good, as a prerequisite *sine qua non* for the development of meaningful interpersonal relations and the functioning of democracy.[89] The ECJ's case law therefore strives to provide a shelter against the "systemic risk" that mass surveillance poses to "the collective European model of liberal democracy".[90] It defends a figure of a citizen who is able to participate freely in a space of genuine social interactions and sustainable democratic practices.

The collective identity conveyed by the ECJ's case law is based on "a personalistic conception of data which has no equivalent in domestic legal orders".[91] Anchored in Articles 7 and 8 of the European Bill of Rights, the ECJ's conception of data privacy (both in *Google Spain* and *Schrems I and II*) places "emphasis on Europe's 'otherness' in relation to the US".[92] Data privacy has thus become "Europe's first amendment", "the main tenet of European constitutional identity",[93] which is promoted within the Union and outwardly projected. *Schrems I and II* lay down "red lines" for the cooperation of EU institutions with third countries, whose conception of privacy is substantially different from that prevailing in Europe. The Court upholds the European data protection paradigm against the threats posed by the laws and practices of such third countries.[94] In this way, European digital citizenship is attached to the territory of the Union, conceived of as a space of values, the integrity of which must be preserved if necessary by not deferring to foreign

88. Opinion in Joined Cases C-293 & 594/12, *Digital Rights Ireland*, para 52. This influence, also known as the "chilling effect", is also underlined by Simon, "Retour des monologues juridictionnels croisés?: À propos de l'arrêt du Conseil d'État dans l'affaire 'French Data'", (2021) *Europe*, Étude 3.

89. See Seubert and Becker, op. cit. *supra* note 87, 31.

90. Dubout, "La Charte et le territoire. A propos de l'effet extraterritorial de la Charte des fondamentaux de l'Union européenne" in Dubout, Martucci and Picod (Eds.), *L'extraterritorialité en droit de l'Union européenne* (Bruylant, 2021), p. 225.

91. Unger, "La souveraineté européenne ou les limites d'un slogan politique", (2021) R.A.E., 579.

92. Petkova, "Privacy as Europe's first amendment", 25 ELJ (2019), 140.

93. Ibid.

94. Although this approach is criticized by Atik and Groussot, "A weaponised Court of Justice in *Schrems II*", 2 *Nordic Journal of European Law* (2021), 1, concluding at 18: "Constitutional values of one party are ill-suited to satisfactorily resolve a legal conflict between two parties. A constitutional court, such as the CJEU – that sees its own law and not that of the counterparty to the conflict – makes reconciliation and resolution far less likely. Europe may 'win' this contest with the United States – and the CJEU's judgment in *Schrems II* may contribute to its policy success. But such a 'win' reflects the exercise of power more than law."

authorities.[95] In a similar manner, the line of case law starting with *Ruiz Zambrano*[96] has established a link between Union citizenship and the territory of the Union, again conceived of as "a space of values", as "a special legal habitat for 'European individuals' deserving of protection".[97] This trend is continued in the body of case law concerning requests by third States for the extradition of Union citizens, starting with the key judgment in *Petruhhin*.[98] By highlighting that in accordance with Article 3(5) TEU, the Union is to contribute to the promotion of its values and the protection of its citizens,[99] the Court alludes to "a conception of protection linked to territory",[100] even if the judgment does not expressly refer to the "territory of the Union" (as in *Ruiz Zambrano*), but to the area of freedom, security and justice. In other words, *Petruhhin* "is rooted in a regard for the rights of the individual that was linked to . . . a certain protective role of the Union legal order over 'its citizens'".[101] Bringing together the "foundational" and the "protective" narratives of the territory of the Union, found respectively in the *Ruiz Zambrano* and in the *Petruhhin* lines of case law, Nic Shuibhne defines the territory of the Union "as a legal place underpinned by common values; and as a place where the EU legal order is engaged to protect Union citizens".[102] The same legal construct appears and assumes a central role in the case law on digital rights, the protection of which connects to the wider interest of defending certain distinctive values of the European polity. If "EU citizenship is intended to promote the feeling of belonging to a community of values that stands up for all its citizens when they cross the external borders of the EU",[103] European digital citizenship has been construed to fulfil exactly the same function when the personal data of the European individuals "travel" outside these borders.

95. Marzal, op. cit. *supra* note 60.

96. Case C-34/09, *Gerardo Ruiz Zambrano* v. *Office national de l'emploi (ONEm)*, EU:C:2011:124.

97. Azoulai, "Transfiguring European citizenship: From Member State territory to Union territory" in Kochenov, op. cit. *supra* note 66, p. 178.

98. Case C-182/15, *Aleksei Petruhhin* v. *Latvijas Republikas Ģenerālprokuratūra*, EU:C:2016:630. For a recent analysis of this body of case law see Mancano, "Trust thy neighbour? Compliance and proximity to the EU through the lens of extradition", 40 YEL (2021), 475.

99. Case C-182/15, *Petruhhin*, para 44.

100. Coutts, "From Union citizens to national subjects: *Pisciotti*", 56 CML Rev. (2019), 521 at 537.

101. Ibid., at 523.

102. Nic Shuibhne, op. cit. *supra* note 35, at 270.

103. Lenaerts and Gutierrez-Fons, "Epilogue on EU citizenship: Hopes and fears" in Kochenov, op. cit. *supra* note 66, at p. 763.

Finally, it is interesting to note, in a similar vein, that in the *Ruiz Zambrano* line of case law, the Court uses the formula of "the substance of the rights"[104] conferred by virtue of Union citizenship status. In *Digital Rights Ireland* and *Schrems I*, the Court develops its understanding of the notion of "essence" of fundamental rights.[105] The terms "substance" and "essence" of rights seem to indicate that what is at stake in these landmark cases on Union citizenship and European digital citizenship is the issue of belonging to a European *ensemble*, defined in axiological terms, i.e. by the adherence to European values.

3. Interplay between the ECJ and other actors

European digital citizenship is evolving as a tapestry woven by several hands. The interplay between the ECJ and national courts, on the one hand (section 3.1), and the EU legislature, on the other hand (section 3.2), is essential. This interplay, sometimes functioning as a driving force and sometimes as a brake, is progressively shaping the contours of European digital citizenship, imbuing it with certain particular features.

3.1. *Interaction with national courts*

The development of European digital citizenship illustrates the reality of judicial dialogue in Europe and the stakes at play. It reveals the degree of maturity that judicial cooperation within the framework of the preliminary reference procedure has reached and the obstacles that it has yet to overcome. Concerning the contribution of national courts, it is again tempting to draw a parallel with the development of the status of Union citizenship, especially in its social dimension. This development has been made possible through the

104. Case C-34/09, *Ruiz Zambrano*, para 42. The formula is consistently reiterated within the line of case law that follows.

105. In *Digital Rights Ireland*, the Court held that generalized (meta)data retention imposed by Directive 2006/24 constituted a particularly serious interference with the right to data protection, but did not affect its essence, as it did not concern the content of electronic communications. In *Schrems I*, the essence of this right is found to be compromised as the US regime also involves access to the content of electronic communications. For a detailed analysis, see Brkan, "The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU's constitutional reasoning", 20 GLJ (2019), 864. The distinction between accessing the content of communications or the metadata has been generally criticized as artificial since the latter can reveal just as much (and even more) sensitive information than the former and is then equally intrusive with respect to e-privacy. The ECJ itself admits in Joined Cases C-203 & 698/15, *Tele2*, para 99, that metadata "provides the means . . . of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications".

interaction between the ECJ and national courts. Commenting on the seminal judgments in *Martinez Sala* and *Baumbast*,[106] the former ECJ judge, Christiaan Timmermans, usefully reminds us of:

> "an element which is often forgotten when wondering why the Court has arrived at a certain interpretation which is considered to be important and innovative. That element is the referral decision of the national court, its motivation and more particularly the content of the preliminary questions themselves. Quite often, a new interpretation given by the Court builds upon the interpretative elements already discussed in the national reference and the arguments submitted by the parties in the main proceedings. It is not rare that it is the question as put forward by the national court and the way in which that question is drafted, which invites the Court to explore new avenues of interpretation and in a way unlocks the door to a new development in the interpretation of Community law."[107]

The observations of Timmermans also apply to the case law on data protection. It is thanks to preliminary references from national courts that cases raising issues of constitutional importance have reached the ECJ. It should be noted that supreme and constitutional courts have stepped into the game from the beginning of the development of digital rights.[108] Their preliminary references do not constitute technical transfer operations by judges seeking to relieve themselves of the responsibility of answering new and thorny questions. Quite the opposite, actually. National courts strategically choose to use the preliminary procedure in order to obtain the advantage of being able to influence the direction taken by the ECJ's case law. Indeed, drawing on their experience and domestic legal traditions, national courts often seek to steer the answers of the Court of Justice; their preliminary reference decisions provide useful and detailed input for possible ways of developing digital rights. In other words, national courts are more and more conscious of the "forward-looking power of the first word"[109] of preliminary

106. Case C-85/96, *Maria Martínez Sala* v. *Freistaat Bayern*, EU:C:1998:217; Case C-413/99, *Baumbast and R* v. *Secretary of State for the Home Department*, EU:C:2002:493.

107. Timmermans, "Martinez Sala and Baumbast Revisited" in Poiares Maduro and Azoulai (Eds.), *The Past and Future of EU Law. The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Hart, 2010), p. 345, at p. 348.

108. From the perspective of institutional dynamics, this is an important difference *vis-à-vis* the developments in the field of Union citizenship.

109. Thym, "Friendly takeover, or: The power of the 'first word'. The German Constitutional Court embraces the Charter of Fundamental Rights as a standard of domestic judicial review", 16 EuConst (2020), 187.

references. Assuming the role of "proactive interlocutors",[110] they are thus claiming their fair share in writing the legal novel on European digital citizenship.

Several examples can be given in this respect. The Irish High Court explained in a convincing manner its doubts on the validity of the secondary law at issue in the complementary cases *Digital Rights Ireland* and *Schrems* (*I and II)*. In the former case, the High Court's reasoning was supported by the contents of a reference from the Austrian *Verfassungsgerichtshof*. As for the French *Conseil d'Etat*, it sought, by formulating numerous and detailed preliminary questions, to influence the definition of the scope of the right to be forgotten.[111] The same French court, together with the Belgian Constitutional Court and the Investigatory Powers Tribunal of London, invited the ECJ to reverse, or at least to limit, the *Tele 2* solution precluding generalized data retention schemes. The call of the national courts was partly heard, since the ECJ introduced an exception on the grounds of safeguarding national security.

Like the case law on Union citizenship, the case law on European digital citizenship illustrates the phenomenon of an "exchange of roles"[112] between the national courts and the ECJ. The former are actively involved in the interpretation and in the shaping of EU data protection law, whereby the latter often determines the final outcome of the case at hand. Still, there are instances in which national courts retain a significant margin of manoeuvre in the application of the ECJ's answer. Such application within the national legal orders determines the effectiveness of European digital citizenship as fleshed out by the ECJ. The national court then becomes the regulator of the real scope of the rights recognized by the ECJ.

A telling illustration of the role of the national court is provided by the reception by the French *Conseil d'Etat*, of the ECJ's judgments in *Google LLC* and *G.C.*, which defined the *territorial* and *material* scope of the right to be delisted. Concerning the former, in its decision of 27 March 2020,[113] the *Conseil d'Etat,* as the highest French administrative court, refused the possibility (opened up by the ECJ) to acknowledge worldwide effects for the obligation to delist, considering that this is not yet required by French law.[114]

110. Odinet and Roussel, "Renvoi préjudiciel: le dialogue des juges décomplexé", (2017) *Actualité Juridique du Droit Administratif*, 740, at 743.

111. See Hardy, "La construction d'un droit européen au déréférencement: De l'importance du dialogue entre la Cour de justice de l'Union européenne et le Conseil d'Etat française", (2020) R.A.E., 407.

112. Kondylis, "The dialogue of judges. National courts and European courts: Case study", 24 *European Review of Public Law* (2012), 83, at 84.

113. CE, 27 mars 2020, *Google-Wikimedia Foundation et Microsoft*, No. 399922.

114. The *Conseil d'Etat* held that "as the applicable law currently stands, it does not follow from any legislative provision that such a delisting could exceed the scope covered by EU law

Concerning the latter, in a series of decisions on 6 December 2019,[115] the French judge drew the necessary consequences from the ECJ's judgment in *G.C.* and established a complete set of guidelines and criteria to be applied by the Commission Nationale de l'Informatique et des Libertés (the French independent authority on data protection) in its future decisions. The approaches of the two courts in this field converge; their dialogue is fruitful with regard to the implementation of the right to be forgotten.

The same cannot be said of the issue of (meta)data retention, which has become the field of a barely concealed confrontation between the two courts. Strong language has been used by the *rapporteurs publics* of the *Conseil d'Etat* to throw into doubt the balance struck by the ECJ's case law. In his opinion leading to the referral decision in *La Quadrature du Net*, the *rapporteur public* Edouard Crépey invited the *Conseil d'Etat* to dismiss a "disciplined" application of a "seriously unbalanced" case law (i.e. *Tele 2*), stating that "the ECJ has incorrectly weighed the different elements of the debate" on (meta)data retention. When the *Conseil d'Etat* had to apply the judgment in *La Quadrature du Net*, the *rapporteur public* Alexandre Lallet advised it to "refuse to transcribe in a servile manner" the Court's solution.[116] He encouraged the *Conseil d'Etat* instead to subject the application of EU law to a conformity check on the basis of the "constitutional safeguard clause". Such a clause includes a series of objectives of constitutional value related to the preservation of public security and to the prevention and combatting of crime.

Following the opinion of the *rapporteur public*, the judgment of the *Conseil d'Etat* in *French Data Network*,[117] which applies *La Quadrature du Net*, draws red lines in the name of the State's mission to guarantee security on its territory, a mission which is constitutionally enshrined. The *Conseil d'Etat* opts for a very broad reading of the exception for national security;[118] in this way, it manages to endorse the essential elements of the French regime of data retention.[119] In other words, *French Data Network* pays lip service to the idea

and be applied outside the territories of the Member States of the EU" (para 10 of the decision of 27 March 2020, *Google-Wikimedia Foundation et Microsoft*, n°399922).

115. CE, 6 décembre 2019, *M. A*, No. 395335; CE, 6 décembre 2019, *M. A*., No. 401258; CE, 6 décembre 2019, *M. A*., No. 405464.

116. The (unusually) lengthy opinion of the *rapporteur public* is published in (2021) *Revue Française de Droit Administratif*, 421. See also the detailed commentary of two members of the Conseil d'Etat: Malvetti and Beaufils, "L'instinct de conservation", (2021) *Actualité Juridique du Droit Administratif*, 1194.

117. CE, Ass., 21 avril 2021, *French Data Network,* cited *supra* note 46.

118. Ibid., para 44.

119. For a more detailed analysis, see in French Iliopoulou-Penot, "La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué", *JCP G*, 14 June 2021, n°24, p. 1152; in English: Christakis, "French Council of

of loyal judicial cooperation by respecting the letter of the judgment in *La Quadrature du Net* while disregarding its spirit. Furthermore, the *Conseil d'Etat* does not hesitate to praise general (meta)data retention,[120] considering it as a decisive factor for the success of criminal investigations and asserting that alternative methods cannot usefully replace it.[121] It openly expresses its disagreement with the ECJ's view on the feasibility and effectiveness of targeted retention[122] and emphasizes the risk that the application of such a method entails for the principle of equality before the law.[123]

In contrast, the Belgian Constitutional Court has faithfully applied the ECJ's judgment in *La Quadrature du Net*.[124] Although the Belgian court had also voiced doubts about the feasibility and effectiveness of targeted retention in its referral decision, it bowed to the ECJ's answer and, in consequence, annulled the obligation of systematic data retention imposed by the Belgian law in question. More importantly, the Belgian Constitutional Court invited the national legislature to elaborate a new regime by adopting the "change of perspective"[125] entailed by *La Quadrature du Net*, with data retention being

State discovers the 'philosopher's stone' of data retention", available at <aboutintel.eu/france-council-of-state-ruling/> (23 April 2021); Vallée and Genevois, "A securitarian solange", *Verfassungsblog* (25 April 2021); Turmo, Op-Ed, "The French Data Network judgment: A 'securitarian Frexit' or classic Conseil d'État Euroscepticism?", *eulawlive* (29 April 2021); Turmo, "National security as an exception to EU data protection standards: The judgment of the Conseil d'État in French Data Network and others", 59 CML Rev., 203–222.

120. It must be noted though that its approach is not necessarily shared by the French Constitutional Court. In its decision of 25 Feb. 2022, in case No. 2021-976/977-QPC, the *Conseil constitutionnel* considered that the provisions of a French law, no longer in force, which provided for indiscriminate (meta)data retention are contrary to the constitutional right of privacy.

121. *French Data Network,* cited *supra* note 46, para 50. In his Opinion in Joined Cases C-511, 512 & 520/18, *La Quadrature du Net*, para 135, A.G. Campos Sanchez-Bordana had addressed this objection as follows: "It is true that the most practical and effective option would involve the general and indiscriminate retention of any data that might be collected by the providers of electronic communications services, but, as I have already said, the issue cannot be settled by reference to what is practically effective; resolving the issue is not a matter of practical effectiveness but of legal effectiveness within the framework of the rule of law."

122. *French Data Network,* cited *supra* note 46, paras. 53 and 54. Such disagreement is echoed in legal commentary. See, e.g. Cameron, op. cit. *supra* note 79.

123. *French Data Network,* cited *supra* note 46, para 54. Interestingly, exactly the same objections, concerning the limited effectiveness of targeted retention as well as the risk it carries to give rise to discrimination, are raised by the Irish Supreme Court in Case C-140/20, *GD*, para 26.

124. Decision of 22 April 2021, *Ordre des barreaux francophones et germanophones*, n° 57/21. See Shipley, "Insight: 'Between Consob and Weiss: The French and Belgian approaches in implementing *La Quadrature du Net*'", *eulawlive* (27 April 2021); Rojszczak, "National security and retention of telecommunications data in Light of recent case law of the European courts", 17 EuConst (2021), 607.

125. Para B 18 of the decision of the Belgian Constitutional Court.

the exception and not the rule. The divergent approaches of the French *Conseil d'Etat* and the Belgian Constitutional Court lead to the fragmentation of the status of the European digital citizen, which clearly does not have the same reach in France and in Belgium.

Furthermore, the right to be defended against indiscriminate surveillance practices continues to encounter national resistance. This is evident in the continuation of the jurisprudential saga on (meta)data retention with three preliminary references, from the Irish Supreme Court,[126] the Federal Administrative Court of Germany,[127] and the French *Cour de cassation*.[128] On 18 November 2021, Advocate General Campos Sanchez-Bordana handed down his Opinion in the three cases, clearly indicating that he did not consider it appropriate for the ECJ to revise its position. He also manifested "a certain irritation with the national courts unwilling to apply clear principles and necessitating more Grand Chamber rulings on this topic".[129] Still, this unwillingness is a strong expression of disagreement by national courts. Such disagreement has probably found support in the different approach of the European Court of Human Rights on the issue of data retention, as manifested in its recent judgments in *Big Brother Watch and others* v. *United Kingdom* and *Centrum för rättvisa* v. *Sweden*.[130] The ECtHR seems to show greater sensitivity than the ECJ to Member States' security concerns.[131] Advocate General Campos Sanchez-Bordana accepts that EU law, as interpreted by the ECJ entails "a more rigorous and stricter regime than the one which emerges from the case law of the ECtHR on Article 8 ECHR",[132] but notes that the level of protection required by EU law on the basis of the Charter may be higher than that of the ECHR in accordance with Article 52(3) CFR.

126. Case C-140/20, *GD*.

127. Pending Joined Cases C-793 & 794/19, *SpaceNet and Telekom Deutschland*.

128. Pending Case C-339/20, *VD and SR*.

129. Woods, "Data Retention: AG Opinions on the latest CJEU cases on national laws", *eulawanalysis* (24 Nov. 2021).

130. ECtHR, Appl. Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch*, cited *supra* note 42, and ECtHR, *Centrum för rättvisa* v. *Sweden,* Appl. No. 35252/08, judgment of 25 May 2021.

131. The ECtHR held that "Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes" (*Big Brother Watch*, ibid., para 347), even if it requires that such regimes be subject to certain "end-to-end" safeguards to prevent arbitrariness and the risk of abuse. The solution of the ECtHR is criticized by Zalnieriute, "Procedural fetishism and mass surveillance under the ECHR", *Verfassungsblog* (2 June 2021). The author considers that the ECtHR "sets a standard, grounded in 'procedural fetishism', which endorses the legality of bulk surveillance operations."

132. Opinion in Cases C-793 & 794/19, *SpaceNet and Telekom Deutschland*, para 39.

In its judgment in *GD* v. *Commissioner of the Garda Síochána*,[133] the ECJ reiterates its principled stance outlawing general (meta)data retention. It also seizes the occasion to answer the double criticism, related to the alleged ineffectiveness of targeted retention in combatting serious crime, as well as the risk of discrimination entailed. This criticism was explicitly formulated by the Irish Supreme Court in *GD* v. *Commissioner of the Garda Síochána* and was also voiced in similar terms by the *Conseil d'Etat* in *French Data Network*.[134] The ECJ considers that "the effectiveness of criminal proceedings generally depends not on a single means of investigation but on all the means of investigation available to the competent national authorities for those purposes",[135] and goes on to explain how targeted retention can be combined with expedited retention and also general detention relating to the civil identity of users of electronic communication and of IP addresses assigned to the source of a connection.[136] It then insists on the possibility for national legislatures to adopt non-discriminatory criteria for the purposes of targeted retention, contributing to the effectiveness of criminal proceedings. It suggests, for example, the targeting of persons who "are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending".[137] The ECJ also recommends the use of a criterion drawn from "the average crime rate in a geographical area", which is likely to concern "both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts" and which is "entirely unconnected with any potentially discriminatory factors".[138] The Court insists above all on the possibility of targeted retention to cover "places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas".[139]

Furthermore, in *GD* v. *Commissioner of the Garda Síochána*, the submission of the Danish Government gives the ECJ the chance to reject the solution of the *Conseil d'Etat* in *French Data Network*. The ECJ considers that where (meta)data retention has exceptionally been retained in a general way for safeguarding national security, "the national authorities competent to undertake criminal investigations cannot access those data in the context of

133. Case C-140/20, *GD*.
134. The submissions of the Irish and French Governments also supported this double criticism.
135. Case C-140/20, *GD*, para 69.
136. Ibid., paras. 70 et seq.
137. Ibid., para 78.
138. Ibid., para 80.
139. Ibid., para 81.

criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purposes of combatting serious crime".[140] Clearly then, the ECJ sticks to its approach in *Tele 2* and *La Quadrature du Net* and shows no intention of taking steps backwards under the pressure exercised by national courts and governments which disapprove of that approach.

Finally, in order to grasp fully the process of the multilevel elaboration of European digital citizenship, it is necessary to examine how national courts apply EU provisions and standards on data protection in cases where they do not refer preliminary questions to the ECJ.[141] A case in point in this respect is provided by the high-profile decisions on the right to be forgotten,[142] in which the *Bundesverfassungsgericht* incorporated the Charter of Fundamental Rights into its standard of constitutional review. In examining whether the ordinary court had correctly carried out the balancing exercise of the fundamental rights at issue, the German Constitutional Court, in its decision *Right to be forgotten II,* took into consideration the ECJ's judgments in *Google Spain* and *GC*.[143] However, it developed a conception of the right to be forgotten that differs in some respects from that promoted by the ECJ, as it attaches greater weight to the freedom of expression and information.[144] The decisions have been read as translating the will of the *Bundesverfassungsgericht* to regain its once eminent position in data protection, catching up with the rise of the ECJ as a key player in this field.[145] A similar intention not to allow the ECJ the leading role in setting the rules of data privacy can be detected in the practice of the *Conseil d'Etat*. In several instances, this French court prefers to interpret important but equivocal provisions of the GDPR on its own, without referring to the ECJ, in order to be able to elaborate the right to data protection in line with the requirements of the domestic legal order.[146] As in other areas of EU law, this leads to inevitable

140. Ibid., para 100. In para 64, the Court already notes that "the fact that traffic and location data were already legally the object of the retention for the purpose of safeguarding national security does not have any bearing on the legality of their retention for the purpose of combatting serious crime".

141. An important source of information in this respect is the general report by Lynskey, and the national reports in Rijpma (Ed.), op. cit. *supra* note 49.

142. Judgments of 6 Nov. 2019, 1 BvR 16/13, *Right to be forgotten I* and 1 BvR 276/17, *Right to be forgotten II*.

143. See Wendel, "The two-faced guardian or how one half of the German Federal Constitutional Court became a European fundamental rights court", 57 CML Rev. (2020), 1383. The author criticizes the choice of the First Senate of the *Bundesverfassungsgericht* not to refer to the ECJ.

144. Friedl, "New laws of forgetting", *europeanlawblog* (12 Dec. 2019).

145. Goldmann, "As darkness deepens: The right to be forgotten in the context of authoritarian constitutionalism", 21 GLJ (2020), 45; Thym, op. cit. *supra* note 109, 187.

146. See the examples given by Teyssedre, "Le droit de l'Union européenne de la protection des données dans le prétoire du Conseil d'État: quels enjeux?", (2021) RTDE, 331.

divergence in the shaping and in the implementation of European digital citizenship. The ECJ still has some way to go to convince national courts to subscribe fully to its constitutional software of protecting e-privacy and to use the preliminary reference procedure as a medium for communication.

3.2. *Interaction with the EU legislature*

The language of fundamental rights and the flagship Articles 7 and 8 CFR have enabled the ECJ to forge a judicial regime of data protection and assert itself not only as a human rights adjudicator, but also as a judge-regulator. The starting point of this trend is *Digital Rights Ireland*, where the ECJ formulated precise instructions for the attention of lawmakers at EU level, concerning the content of future secondary law.[147] The trend is pursued in *Tele 2* and in *La Quadrature du Net*, indicating what national regulators can (and cannot) do in the name of security in the design of data retention regimes. *La Quadrature du Net* sets out a detailed "user manual" in this respect. This judgment contains a graduated system of "acceptable" breaches with regard to e-privacy, taking into account the specific purposes pursued by national authorities, the nature of the data concerned and the type of retention measures.[148]

As the ECJ itself explains in the subsequent judgment in *GD* v. *Commissioner of the Garda Síochána*, it has established, in accordance with the principle of proportionality, "a hierarchy" among the different public interest objectives related to security issues,[149] with the objective of safeguarding *national security* situated on top of the list (and thus being capable of justifying measures entailing the most serious interferences with fundamental rights, such as general retention of metadata other than IP addresses). In the same judgment, the Court suggests the use of certain geographical criteria for data retention, such as the targeting of areas with a high instance of crime or volume of visitors, as well as locations which house critical infrastructures. The issue of data retention has then clearly led the Court to make choices of a legislative nature. In a similar manner, the very recognition of the right to be forgotten and the definition of how it is to be

147. Granger and 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", 39 EL Rev. (2014), 835.

148. General and indiscriminate retention of (meta)data other than IP addresses is possible only when a State is confronted with a serious threat to national security, that is shown to be genuine and present or foreseeable, for a period limited in time to what is strictly necessary, but which may be extended if that threat persists. On the other hand, the purposes of combatting serious crime and preventing serious threats to public security can only give rise to measures of targeted retention, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion.

149. Case C-140/20, *GD*, para 56.

implemented in practice have turned the ECJ into an essential author of EU law on data protection. Indeed, it should be recalled that Directive 95/46 (applied in *Google Spain)* did not mention the specific issue of delisting by search engines.

The question then inevitably arises: has the ECJ crossed the lines drawn by the separation of powers within the constitutional order of the Union? Has it made choices that are normally incumbent upon the legislature? This is reminiscent of the question of the "proper" relationship between the EU judiciary and the legislature in the development of Union citizenship.[150] It also recalls the criticism levelled at the pioneering case law in this field, which was that, through the interpretation of general and indeterminate provisions of primary law, the Court elaborated outcomes which should normally be articulated under the responsibility and within the framework of the legislative process. In order to discuss such criticism, it is necessary briefly to examine the EU legislature's role in the field of data protection.

Data regulation was initially approached through the prism of the market, before being "conquered" by the logic of guaranteeing individual rights (with the market logic remaining present). Thus, Directive 95/46, which was adopted on the basis of the harmonization clause of the internal market (current Art. 114 TFEU), aimed to ensure and to increase, in view of their economic value, the cross-border flow of data, by, *inter alia*, preventing Member States from relying on national data protection laws in order to limit their free movement. The Lisbon Treaty introduced a change of paradigm in this field. By establishing an autonomous legal basis for the adoption of secondary law on data, i.e. Article 16(2) TFEU, it explicitly recognized the need for legislative intervention in order to give effect to the right to data protection. This right is enshrined in Article 16(1) TFEU, and labelled as fundamental by its inclusion in Article 8 CFR. The Treaty then gives a mandate to, and even creates a duty for, the EU legislature to lay down rules that concretize the right to data protection.[151] In other words, the role of the legislature consists in "defining the arrangements for exercising this right

150. The dynamics of the legislative-judicial interplay have constituted an important tool for analysing the development of Union citizenship as shown by Nic Shuibhne, "The third age of EU citizenship. Directive 2004/38 in the case law of the Court of Justice" in Syrpis (Ed.), *The Judiciary, the Legislature and the EU Internal Market* (Cambridge University Press, 2012), p. 331, and by Wollenschläger, "The judiciary, the legislature and the evolution of Union citizenship" in the same collection, p. 302. Also see Syrpis, "The relationship between primary and secondary law in the EU", 52 CML Rev. (2015), 461.

151. Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Article 16 TFEU* (Springer, 2016), especially Ch. 5, "Understanding the scope and limits of the EU legislator's contribution to the mandate under Article 16 TFEU", pp. 263 et seq.

more precisely, in order to ensure that individuals can enjoy it effectively".[152] The adoption of the GDPR is fully in line with this perspective.[153] This normative instrument is an emblematic illustration of the function of the EU legislature, consisting in giving concrete expression and practical effect to fundamental rights.[154] It constitutes a unique regulatory framework for data privacy, and can be seen as a legislative success story in this field. Indeed, the GDPR

> "carried forward the legacy of the Data Protection Directive, which it replaced, by insisting on the same core principles of European data protection law, and codified some of the case law that the Court of Justice had rendered in the interim. But it also injected new concepts and ideas into European data protection law and reformed its institutional structure".[155]

All of the GDPR is driven by a particular philosophy and a compelling objective: to ensure that Europeans maintain control over their data.[156] Inspiration for this foundation of EU data protection law was drawn from the "right to informational self-determination",[157] which originated in the case law of the German Constitutional Court[158] and was later taken up by the

152. Tinière, "L'apport de la Charte des droits fondamentaux à la protection des données personnelles dans l'Union européenne", (2018) R.A.E., 32.

153. The political battles surrounding the adoption of the GDPR are captured in David Bernet's film "Democracy. *La ruée vers des datas*" which follows two key figures of these battles: the rapporteur for the European Parliament, Jan Philipp Albrecht and EU Commissioner Viviane Reding.

154. Lorans, "Le législateur européen et la protection des droits fondamentaux dans l'Union: vers une concrétisation législative de la Charte", (2021) RTDE, 59.

155. Streinz, "The evolution of European data law" in Craig and de Burca (Eds.), *The Evolution of EU Law*, 3rd ed. (OUP, 2021), p. 902.

156. On the important role of "individual control" in EU data protection law see Lynskey, *The foundations of EU Data Protection Law* (OUP, 2015), especially Part II. The EU legislature's objective to ensure "individual control" resonates with the aspiration of European citizens expressed by the Conference on the Future of Europe (Plenary), Proposal 34 Safe and trustworthy digital society data protection, "We promote data sovereignity of individuals, better awarness and more efficient implementation and enforcement of existing data protection rules (GDPR) to enhance personal control of own data and limit misuse of data", at <futureu.europa.eu/pages/plenary?locale=en>.

157. On this right, see Rouvroy and Poullet, "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy" in Gutwirth, Poullet, de Hert, de Terwangne and Nouwt (Eds.), *Reinventing Data Protection?* (Springer, 2009), p. 45; Türk, "L'autodétermination informationnelle: un droit fondamental émergent?", (2020) *Dalloz IP/IT*, 616.

158. BVerfG, 15 Dec. 1983, 1 BvR 209/83. This right was understood by the German Constitutional Court as being "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life

ECtHR.[159] Thus, the will to guarantee one's ability to control the traces one leaves in the digital environment and, therefore, to remain master of one's digital identity becomes a structural principle of the GDPR.[160] Expressed in Recitals 7, 68, 75 and 85 of the GDPR, this principle makes the individual's consent the centrepiece of the regime and constitutes the foundation of several specific rights, such as the right of access, the right to rectification, the right to erasure, the right to data portability, and the right to object.[161] In its first report on the application of the GDPR, the Commission presented "data protection as a pillar of citizens' empowerment".[162]

The philosophy of individual empowerment also underpins the case law on European digital citizenship. It is conveyed by the recognition of the right to be delisted, which in principle prevails not only over the commercial interest of the operator of the search engine, but also over the general public's interest to access information. This right enables an individual to determine the fate of information displayed lawfully and appearing in the list of results associated with his/her name. Furthermore, the ECJ's case law on (meta)data retention (or rather its prohibition) embodies the logic of control by the individual, who remains the *subject* of rights; it opposes the individual's transformation into the *object* of generalized surveillance.[163] This case law also materializes the "principle of purpose limitation",[164] a core element of EU law on personal data which protects individuals from risks of misuse and abuse of data bases. This principle, enshrined in Article 8 CFR, is set out in detail in Article 5(1)(b) of the GDPR: "Personal data shall be . . . collected for specified, explicit and legitimate purposes and not further processed in a manner that is

should be communicated to others". For an analysis of the decision of 1983, see Hornung and Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination", 25 *Computer Law and Security Report* (2009), 84.

159. The ECtHR held that "Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged"; ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy* v. *Finland,* Appl. No. 931/13, judgment of 27 June 2017, para 137; ECtHR, *Benedik* v. *Slovenia*, Appl. No. 62357/14, judgment of 24 April 2018, para 103.

160. Eynard, "RGPD et 'empouvoirement' individuel: promesse tenue ou espoir déçu?" in Castets-Renard (Ed.), *RGPD, cinq ans après*, (2021) R.A.E., 15.

161. Set out in Arts. 15, 16, 17, 20 and 21 GDPR.

162. COM(2020)264 final, Communication from the Commission to the European Parliament and the Council, 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.

163. See Azoulai and Ritleng, "'L'État, c'est moi'. Le Conseil d'État, la sécurité et la conservation des données", (2021) RTDE, 341.

164. Ibid.

incompatible with those purposes".[165] It thus seems that the ECJ's case law had at first anticipated the adoption of the GDPR. The Court then integrated the principles and objectives outlined by the EU legislature, and even extended them further.

Nevertheless, the fact remains that the ECJ's case law on (meta)data retention has been and continues to be subject to considerable reservations. This probably explains why the political process has taken over the issue. This is evidenced by the ongoing discussion of the draft Regulation on Privacy and Electronic Communications (the E-Privacy Regulation).[166] Presented in 2017, this proposal aims to replace the regime resulting from Directive 2002/58. After three years of deadlock within the Council, due to the diverging views of the Member States, the Portuguese presidency (first semester of 2021) decided to relaunch the discussions. The compromise text finally released on 10 February 2021[167] includes two provisions which have raised eyebrows, as they clearly diverge from the ECJ's case law. Indeed Article 6(1)(d) and Article 7(4), authorize the processing of data and retention of metadata, respectively, "in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security".[168] The European Data Protection Board expressed concerns over these provisions in

165. See the commentary of this provision by de Terwangne in Kuner, Bygrave, Docksey and Dreschler (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP, 2020).

166. COM(2017)10 final, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 Jan. 2017.

167. Document 6087/21 of the Council, Mandate for negotiations with the European Parliament, 10 Feb. 2021. Trilogue meetings began on 20 May 2021, but without significant progress since.

168. More precisely, under Art. 6(1)(d), "Providers of electronic communications networks and services shall be permitted to process electronic communications data only if . . . it is necessary for compliance with a legal obligation to which the provider is subject laid down by Union or Member State law, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security." Under Art. 7(4), "Union or Member state law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists."

its statement of 9 March 2021, and invited the EU legislature not to derogate from the ECJ's judgment in *La Quadrature du Net*.[169]

In addition to the discussions on the draft E-Privacy Regulation, in February 2021, a number of Member States supported the idea of adopting EU legislation harmonizing the legal regime for data retention for law enforcement purposes. In June 2021, the Commission invited Member States to present their views on this issue "in light of the Court's case law".[170] The Commission suggested three possible approaches: first, refraining from any EU initiative, and leaving the States to address the consequences of the Court's case law for their legislation, with due account for national specificities; second, issuing guidance and recommendations; third, presenting a legislative initiative, which could either be comprehensive, i.e. covering the retention of all (meta)data categories[171] and for all purposes,[172] or limited to specific data categories and/or specific purposes. In the views presented, a majority of Member States seems in favour of the adoption of a new European regime, but with important differences concerning its substance.[173] Progress in the legislative arena is then bound to be slow, while the Court continues to provide guidance concerning (meta)data retention, further limiting the margin of *manoeuvre* enjoyed by the lawmakers at EU as well as national level. For example, in *GD* v. *Commissioner of the Garda Síochána*, the Court rejected any blurring of the line between national security and serious crime, considering that "criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security",[174] contrary

169. European Data Protection Board, Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021: "the ePrivacy Regulation cannot derogate from the application of the latest CJEU case law, which notably provides that Articles 7, 8, 11 and 52(1) of the Charter must be interpreted as precluding legislative measures, which would provide, as a preventive measure, the general and indiscriminate retention of traffic and location data. Therefore, providing a legal basis for anything else than targeted retention for the purposes of law enforcement and safeguarding national security is not allowed under the Charter, and would anyhow need to be subject to strict temporal and material limitations as well as review by a Court or by an independent authority."

170. Document 6455/21 of the Council, Retention of electronic communication data – exchange of views, 2 March 2021.

171. I.e. traffic and location data, IP addresses.

172. I.e. national security, serious crime/serious public security threats, general crime/public security threats.

173. Several national responses to the Commission's questions are available at <www.statewatch.org/news/2021/december/eu-data-retention-strikes-back-options-for-mass-telecoms-surveillance-under-discussion-again>.

174. Case C-140/20, *GD*, para 63. At para 62, the Court observes that "unlike crime, even particularly serious crime, a threat to national security must be genuine and present, or, at the very least, foreseeable, which presupposes that sufficiently concrete circumstances have arisen to be able to justify a generalized and indiscriminate measure of retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its

to the Commission's submission. It is clear then that the Court's case law, guaranteeing individual rights and conveying a demanding conception of data privacy, will frame more and more tightly public regulatory responses to the issue of (meta)data retention.

One final question remains. If the E-Privacy Regulation and an eventual harmonized regime on data retention are adopted, what will be the fate of the provisions eventually authorizing indiscriminate (meta)data retention for purposes other than national security if the ECJ is seized of an action for annulment or of a preliminary reference on their validity? Will it opt for confrontation by censuring the EU legislature, or will it show deference to the choices made through the legislative process? In other words, how will the enactment of secondary law affect the Court's reading of primary law? It may be useful to recall that the adoption of Directive 2004/38[175] entailed an important change in the Court's case law on the social dimension of Union citizenship. In fact, the ECJ showed deference to the States' interests and steered its interpretation of primary law in order to align it with the preferences of the EU legislature.[176] It will be interesting to see whether a similar phenomenon will take place following the (eventual) adoption of new European rules on e-privacy and (meta)data retention. Of course, much will depend on the political context which necessarily influences the Court's approach, be it dynamic or restrained.

4. Conclusion

Taking ownership of the Charter of Fundamental Rights in the case law on personal data and privacy, the Court has consecrated two important rights of the data subject: the right to be delisted and the right to be defended against practices of mass (meta)data retention. Our reading of this case law highlights the emergence of a protective and empowering status for the individual in the face of both corporate and State power. This status is linked to the territory of

seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed".

175. Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, O.J. 2004, L 158/77.

176. Case C-158/07, *Jacqueline Förster* v. *Hoofddirectie van de Informatie Beheer Groep*, EU:C:2008:630; Case C-333/13, *Dano*, EU:C:2014:2358; Case C-299/14, *Vestische Arbeit Jobcenter Kreis Recklinghausen* v. *Jovanna García-Nieto and others*, EU:C:2016:114; Case C-67/14, *Jobcenter Berlin Neukölln* v. *Nazifa Alimanovic and others*, EU:C:2015:597.

the Union, conceived as a special space of values, which embodies a highly demanding conception of data privacy. This conception shapes membership of a European *ensemble* and is worth defending against the outside. It is then possible to describe the status based on data privacy as an embryonic European digital citizenship, aiming to ensure that the autonomy and integrity of the individual in the digital ecosystem is not weakened, but reinforced.

Conceptualizing the new set of digital rights as a European digital citizenship widens our understanding of citizenship within the EU legal order, beyond the paradigm based on the rights of Member State nationals to move within and to remain in the territory of the Union. A more elaborate picture unfolds within which Union citizenship stands at the centre of the EU's universe of rights, with other statuses (often including third-country nationals residing in the EU) evolving next to it. European digital citizenship is one of them. It grows parallel to and implicitly draws inspiration from the development of the "fundamental status" of Union citizenship, based on Articles 20 and 21 TFEU. The institutional trajectory along which it develops presents several commonalities with the one which has shaped Union citizenship. In both cases, evolution is strongly driven by the Court of Justice, interpreting primary law as a constitutional source of individual rights and not hesitating to legislate through case law. The input of national courts, displaying both cooperative attitudes and resistance, has also been significant in the construction of Union citizenship and European digital citizenship. Both case law edifices resulting from the dialogue between the ECJ and national courts are underpinned by a common conception of the European individual as a subject empowered and protected by the EU legal order, and of the territory of the Union as a distinct geographical, legal, and normative space.

The judiciary is of course by definition only one of the actors of the "institutional pluralism"[177] that commands the constitutional trajectory of the Union. As a consequence – and as is also the case with Union citizenship – the main features of European digital citizenship cannot be designed solely through judicial interpretation. The EU legislature's participation in outlining its contours as well as in shaping the internet as a rights-respecting public space remains essential. Indeed, the EU legislature is well suited to taking a global overview of the reconfiguration of the relationship between public authorities, big tech companies and individuals, whereas the ECJ can only

177. See Davies, "Legislative control of the European Court of Justice", 51 CML Rev. (2014), 1579: "The constitution should be the property of all those with a stake in its outcomes, and this philosophical starting point should express itself legally in a situation which may be described in terms of institutional pluralism, or non-dominance, with neither courts nor legislatures able to make their view of the constitution the only one that counts."

answer specific questions, depending on the cases that come before it (especially through preliminary references). Moreover, the EU legislature is able to formulate an understanding of the new status conciliating diverging Member States' conceptions and taking into account other – potentially competing – demands placed high on the political agenda of the EU.[178] The adoption of the GDPR and of the Digital Services Act[179] as well as the ongoing discussion of the proposed E-Privacy Regulation and of a possible European regime on (meta)data retention show that the EU legislature is aware of the need to take part in "the EU response to the potential threat of the digitalization of the society and its extraordinary potential for control".[180] Legislative measures then usefully complete the judicial application of the Charter as a tool of "limited digital governance"[181] and participate, along with it, in the movement to develop a digital citizenship. This form of citizenship addresses access to the digital world as a common good and guarantees the individual's ability to act and interact freely and meaningfully in the online dimension of society.

Defending such a vision, and with EU law on data protection already benefiting from a globalizing effect,[182] also known as the "Brussels effect",[183] the EU can clearly provide useful input in the global debate on the place of the individual in the information society.[184] It should be recalled that the internal market equips the EU with the power to act as a "responsible global leader of

178. As an anonymous reviewer has rightly pointed out, given the high carbon demands of the information society, more joined-up thinking and action is needed about what the different facets of European citizenship (digital, environmental, etc.) mean and require.

179. On 23 April 2022, Thierry Breton announced that the European Parliament, the Council of the EU and the Commission had agreed on the adoption of the text proposed less than 18 months earlier (COM(2020)825 final, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 Dec. 2020), available at <www.linkedin.com/pulse/against-all-odds-making-internet-safer-place-digital-services-breton/>.

180. Groussot, Zemskova and Gill-Pedro, "Towards general principles 2.0: The application of general principles of EU Law in the digital society" in Bernitz, de Vries, Groussot and Paaju (Eds.), *General Principles of EU Law and the EU Digital Order* (Kluwer, 2020), p. 478.

181. Ibid.

182. See Streinz, op. cit. *supra* note 155, p. 902, at p. 931: "The expanded scope of application of EU data protection law, its extending through unilateral adequacy assessments and other safeguards, and the promoting and defending of the EU's conception of data protection and privacy in international instruments have all contributed significantly to the globalisation of European data protection law."

183. Bradford, *The Brussels Effect: How the EU Rules the World* (OUP, 2020).

184. The Declaration for the future of Internet, endorsed on 28 April 2022 by the EU, the US and several other international partners, which sets out the vision of a safe and trustworthy internet, is a first small step in the right direction. See <ec.europa.eu/commission/presscorner/detail/en/IP_22_2695>.

a human-centred and value-based approach model in the digital age"[185] in the face of US dominance in digital technologies, which should not be considered as a "fatalité" imposed on Europeans. The challenges and risks raised by the use of digital technologies may prompt the EU to advance further in the direction of developing a digital European sovereignty destined to defend European digital citizenship.

185. COM(2022)27 final, cited *supra* note 2, p. 7.