White Rose Research Online

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk
Universities of Leeds, Sheffield and York

Deposited via The University of Sheffield.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/214033/

Version: Published Version

Article:
Tzanou, M. and Vogiatzoglou, P. (2025) National security and new forms of surveillance: from the data retention saga to a data subject centred approach. European Papers, 10 (3). pp. 803-836. ISSN: 2499-8249

https://doi.org/10.15166/2499-8249/855

This is a pre-copyedited, author-produced version of a paper accepted for publication in European Papers – A Journal on Law and Integration (www.europeanpaper.eu) following peer review. The final version of the paper, National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach will be available on-line at: https://www.europeanpapers.eu/

Reuse
This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs (CC BY-NC-ND) licence. This licence only allows you to download this work and share it with others as long as you credit the authors, but you can't change the article in any way or use it commercially. More information and the full terms of the licence here: https://creativecommons.org/licenses/

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

UNIVERSITY OF LEEDS
University of Sheffield
UNIVERSITY of York

European Papers – A Journal on Law and Integration
Vol. 10, No. 3, 2025, pp. 803–836

The Future of Digitalisation in EU Law Enforcement
edited by **Niovi Vavoula**

National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach

Maria Tzanou[*] *and Plixavra Vogiatzoglou*[**]

TABLE OF CONTENTS: 1. Introduction. – 2. National Security. – 2.1. Definition and Scope. – 2.2. Private Sector and the Expanding Application of EU Law. – 3. The Legal Uncertainty Arising from the Current Delineation of the Scope of EU Data Protection Law. – 3.1. Narrowing the Scope Back Down? The Draft E-Privacy Regulation. – 3.2. National Security and New Forms of Surveillance. – 3.3. Grounding EU law applicability on secondary law interpretations – 4. Rethinking the Scope of Application of EU Law in the Context of National Security: A new approach. – 4.1. National security through the prism of digital constitutionalism. – 4.2. A new data-subject-centric model. – 4.3. Normative foundation and the benefits of the data-subject model. – 4.4 Addressing the Objections to the data-subject model. – 5. Conclusions

ABSTRACT: National security is a regulatory complex area that brings together public and private actors performing a variety of functions for the safeguarding of the EU Member States' national interests. The article critically reflects on the applicability of EU law in this area by examining the complexities and controversies surrounding the respective judiciary and legislative approaches as well as the emerging surveillance practices deployed under the veil of national security. It argues that, while it is laudable that some aspects of national security were brought within the scope of application of EU law by the CJEU through its data retention jurisprudence, the grounding of the EU law applicability on the activities of private entities (controllers) is problematic. In particular, it creates significant legal uncertainties as private and public bodies are increasingly intertwined in the field of security and Member States push back against such expansion of EU law, while the case law does not take into account new forms of intrusive surveillance such as Pegasus. To counter these issues, the article proposes a new *data subject-focused* approach for the grounding of the scope of application of EU law -including to national security measures- which shifts the focus

[*] Senior Lecturer, School of Law, University of Sheffield, UK, m.tzanou@sheffield.ac.uk..
[**] Postdoctoral researcher UvA ACIL – IViR, Affiliated senior researcher KU Leuven CiTiP, p.a.vogiatzoglou@uva.nl.

The drafting of sections 3.2, 3.3 and 4 is attributed to Maria Tzanou, and that of sections 2 and 3.1 to Plixavra Vogiatzoglou. Sections 1 and 5 were co-drafted. The whole manuscript is shaped by both authors. The paper was tentatively accepted in April 2024, since then minor revisions have been made, and the Special Section was accepted in June 2025.

ISSN 2499-8249
doi: 10.15166/2499-8249/855
www.europeanpapers.eu
(CC BY-NC-ND 4.0)

from the entity carrying out the national security operation (controller) to the individuals being affected (data subject). As such, it aligns better with fundamental rights and the constitutional foundations of EU data protection law and is urgently needed in the rapidly privatised and algorithmised area of national security.

KEYWORDS: national security – data retention – EU data protection law – algorithmic surveillance – digital constitutionalism – Pegasus.

1. Introduction

The increased privatisation and algorithmisation of Member States' national security through the deployment of emerging technologies, such as machine learning, Artificial Intelligence (AI) and modern spyware, pose unprecedent risks to EU fundamental rights. New forms of digital surveillance have been deployed by EU Member States, such as Pegasus, which is considered 'the most powerful hacking tool or spyware'[1] developed to date granting 'complete, unrestricted access' to the targeted mobile phones, and all the information contained on these.[2] Member States's national governments are increasingly procuring powerful spywares and data mining and predictive tools by private tech companies, such as Palantir considered to be involved in 'serious human rights abuses' worldwide.[3]

Yet, the scope of application of EU law in this area remains unclear and convoluted. Pursuant to Article 4(2) of the Treaty on European Union (TEU), 'national security remains the sole responsibility of each Member State'. In the now (in)famous *Privacy International* and *La Quadrature du Net* (LQdN) rulings, the Court of Justice of the EU (CJEU) established that activities by electronic communications services providers (ECSPs), carried out for national security purposes, are subject to EU law, while activities by intelligence services alone are exempted.[4] Nevertheless, there are significant uncertainties about the applicability of such distinctions in practice, due to the blurred boundaries between national and public security and even more so where the involvement of private actors in national security surveillance goes beyond the activities of ECSPs and includes new forms of surveillance, such as Pegasus.[5]

[1] European Data Protection Supervisor, Preliminary Remarks on Modern Spyware, 15 February 2022, at www.edps.europa.eu 3.

[2] D Pegg and S Cutler, 'What is Pegasus Spyware and How Does it Hack Phones?' (The Guardian, 18 July 2021), at www.theguardian.com.

[3] A Bychawski, 'What you need to Know about Palantir, the US Firm in Line for a £480m NHS Deal' (Open Democracy, 23 October 2023) at www.opendemocracy.net.

[4] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier minister and Others* EU:C:2020:791.

[5] Pegg and Cutler (n 2).

Furthermore, the EU legislator has increasingly been pursuing a different approach to the regulation of national security activities, as demonstrated for instance by the freshly agreed upon AI Act. Accordingly, the AI Act shall not apply to national security regardless of the actor involved, contrary to the CJEU's jurisprudence.[6]

This article aims to contribute to this debate and advance legal certainty by offering a new way of thinking how the exercise of power in the context of national security ought to be limited and made subject to review in the EU digital ecosystem. This approach considers the applicability of EU fundamental rights to national security measures as a pre-condition for the achievement of the constitutional equilibrium in this area, without which the substantive fundamental rights protection cannot be realised.

The article makes two distinct contributions to the debate of EU regulation of national security: First, it investigates the complexities and controversies surrounding the scope of application of EU law to national security surveillance. In this regard, it argues that, while it is laudable that some aspects of national security were brought within the scope of application of EU law by the Court through its data retention jurisprudence, the grounding of the EU law applicability on the activities of private entities (controllers) is problematic because it creates significant legal uncertainties. To demonstrate this, we first expose the issues raised by this case-law and its legislative aftermath. Then, we employ two case studies of surveillance measures deployed by EU Member States: data mining and analysis software developed by Palantir and the Pegasus spyware surveillance. Second, situating the discussion within the digital constitutionalism framework, the article proposes a new way of thinking about this topic, a *data-subject centric* model for establishing the applicability of EU fundamental rights law to national security which aligns better with the constitutional foundations of EU data protection law.

This is the first time that such an approach is developed and proposed in the academic field. To date, academic literature has mainly focused on discussing national security in relation to the Court's data retention case law.[7] A discussion on new forms of surveillance, such as Pegasus is emerging and focuses primarily on

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Art 2(3).

[7] See for example M Rojszczak, 'National Security in a Digital Europe' (2023) 48 *European Law Review* 544. By contrast, see P Vogiatzoglou and S Fantin, 'National and Public Security within and beyond the Police Directive' in A Vedder, J Schroers, C Ducuing and P Valcke (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructures* (Intersentia 2019) 27.

demonstrating their unprecedent risks on fundamental rights.[8] However, this discussion is limited if EU fundamental rights are barred from applying to the use of such surveillance systems in the area of national security. Privacy scholars, such as Korff, have called for national security agencies to be made subject to EU law and the EU Charter of Fundamental Rights (Charter).[9] Their arguments are normally based on the Court's expansive data retention case law. However, the data subject model, proposed here, differs from these analyses for two reasons. First, we call for a general shift from the focus on controllers to data subjects when establishing the applicability of EU law in the national security context. Second, we argue that there is a principled, theoretically and doctrinally more robust framework to achieve this, inspired by digital constitutionalism, which differs from what has already been proposed in the case law, by regulators and debated in academic legal scholarship.

Legal certainty is urgently needed in the rapidly privatised and algorithmised area of national security.[10] The lack of applicability of EU fundamental rights law on national security measures and on new forms of surveillance procured by Member States is an issue that has significant repercussions for collective and individual level protections in the EU even if the CJEU has expanded the application of EU law in the area. The rethinking of the issue of grounding the application of EU law as proposed in the article is likely to influence academic debates in the area, and more importantly, to produce practical consequences. It aims to demonstrate to the EU legislator and the judiciary that there is a different way to approach this issue, which breaks free from current constraints, uncertainties and shortcomings. If such an approach were to be adopted by the EU legislator or the judiciary, then new surveillance forms (such as Pegasus) would no longer fall outside the scope of EU fundamental rights law.

The article is structured as follows: Section 2 examines the national security activities that fall within the scope of EU law. It critically discusses the distinction between national and public security and the CJEU's development of what can be characterised as a data *controller-focused approach*, which relies primarily on the role of the private sector for expanding the applicability of EU (data protection) law onto national security operations. Section 3 challenges this approach, by demonstrating the fragmented responses by the EU legislator following the CJEU's jurisprudence and on the basis of two case studies of new surveillance forms: Palantir and Pegasus. It argues that the controller-focused approach is subject to conflicting interpretations that neglect the

[8] See for example G Sartor and A Loreggia, 'The Impact of Pegasus on Fundamental Rights and Democratic Processes' (European Parliament, January 2023) at www.europarl.europa.eu.

[9] D Korff, 'Opinion on the Implications of the Exclusion from New Binding European Instruments on the Use of AI in Military, National Security and Transnational Law Enforcement Contexts' (European Center for Not-for-Profit Law, October 2022) at ecnl.org.

[10] R Jansen and M Reijneveld, 'Convention 108+, the GDPR, and Data Processing in the National Security Domain' (2022) 8 *European Data Protection Law Review* 423.

working reality of intelligence services and the increasing use of emerging technologies which bring novel risks to fundamental rights and the EU democratic society. Section 4 proposes a novel, *data subject-centric* model, which could yield a higher degree of legal certainty, coherence and protection of individuals rights and freedoms than the one currently followed in the EU. The analysis addresses the potential objections to this model and considers possible ways to overcome these *de lege lata* and *de lege ferenda*. The final section contains concluding remarks.

2. National security

2.1. Definition and scope

Under Article 4(2) of the Treaty on European Union (TEU), 'national security remains the sole responsibility of each Member State'.[11] Conversely, other aspects of security, such as the safeguarding of public security and the fight against crime, fall within the scope of EU law.[12] However, the concept of national security is not delineated in EU law, nor is there a single unilaterally accepted definition.[13] Moreover, public security has been expanding into a notion overlapping or even being assimilated to national security.[14] Therefore, discerning what constitutes an activity in pursuit of national security becomes an increasingly complex task.

National security, often also referred to as state security in case law and legislation, seems linked to the core sovereignty and democratic nature of the state, relating to both internal and external dimensions of security.[15] In *Privacy International* and *LQdN*, the CJEU described the national security responsibility incumbent upon Member States under Article 4(2) TEU as corresponding: 'to the primary interest in protecting the *essential functions of the State and the fundamental interests of society* and [as encompassing] the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social

[11] See also P Vogiatzoglou, 'The Era of Pre-Crime: How Mass Data Surveillance and Predictive Policing Intersect and Interfere with Privacy, Data Protection and Due Process Rights in the EU' (KU LEUVEN, 2023), at lirias.kuleuven.be.

[12] Treaty on the European Union [2016], Art 3(2); Title V of the Treaty on the Functioning of the European Union [2016].

[13] Vogiatzoglou and Fantin (n 7).

[14] Ibid. 42, 47.

[15] See for example Case C-285/98 *Tanja Kreil v Bundesrepublik Deutschland*, EU:C:2000:2, para 17; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Arts 1(3) and 15(1). See also P Koutrakos, *Exceptions from EU Free Movement Law: Derogation, Justification and Proportionality* (Hart Publishing 2016) 190; Vogiatzoglou and Fantin (n 7).

structures of a country and, in particular, of directly *threatening society, the population or the State* itself, such as *terrorist activities*'.[16]

At the Council of Europe (CoE) level, national security is broadly subject to scrutiny and regulation. First, the European Court of Human Rights (ECtHR) is competent to scrutinise state measures pursuing the aim of national security.[17] Although the ECtHR may recognise a wider margin of appreciation to states when examining the proportionality of national security measures, given its powers in this context, it has neither defined national security nor does it always distinguish between national and public security.[18] Ultimately, the Court equally endorses a restrictive interpretation of national security, stating that its limits cannot 'be stretched beyond its natural meaning'.[19] Second, the CoE Convention on data protection (Convention 108+) enables Contracting States to apply the rules therein to all sorts of processing activities, including state security. It further foresees permissible restrictions to its rules for national security purposes, which must, however, abide by certain conditions.[20] Finally, the CoE Recommendation on data processing by police explicitly recognises that states may extend the applicability of those international data protection rules and principles also to the field of state security.[21]

At the EU legal order, the national security exception raises more complex issues. In this context, national security (which falls outside the scope of EU law) may be juxtaposed to public security which falls within the scope of EU law. Public security appears to be linked to the internal security of a state, as well as the security of the

[16] *Privacy International* (n 4) para 74; *La Quadrature du Net and Others* (n 4) para 135. However, when discussing the purpose of the fight against terrorism pursued by the PNR Directive, the CJEU was much less willing to accept that it may also include monitoring activities by intelligence and (national) security services. Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministers*, EU:C:2022:491 para. 236, on Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[17] See for example European Convention on Human Rights [1950], Art 8(2).

[18] See for example *Centrum för Rättvisa v. Sweden* App n. 35252/08 (ECtHR, 19 June 2018) para 112. See also N Ní Loideain, *EU Data Privacy Law and Serious Crime: Data Retention and Policy-making* (Oxford University Press 2023) 61; M Rojszczak (n 7) 549.

[19] *Case of C.G. and Others v. Bulgaria* App n. 1365/07 (ECtHR, 24 April 2008) para 43.

[20] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) [1981, 2018] Arts 3(1), 11 and II Commentaries point 47. See also P Vogiatzoglou, 'Article 2: Scope' in E Kosta, F Boehm (eds), *The Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024) 67.

[21] Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, Explanatory Memorandum point 29 [1987].

European public, its citizens and the EU territory.[22] Furthermore, the definitions given to public security within case law and secondary law start to closely resemble the above description of national security. For instance, the CJEU has stated that public security could be affected by 'a threat to the *functioning of the institutions and essential public services and the survival of the population*, as well as the risk of a serious *disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests*'.[23] This definition has been further endorsed within secondary (data protection) law, whereby public security is considered to '[presuppose] the existence of a *genuine and sufficiently serious threat* affecting one of the *fundamental interests of society*', such as those described in the above case law.[24] Finally, terrorism constitutes a serious crime within the broader realm of security for which the EU is co-responsible.[25]

The references to fundamental interests of society, essential services, survival of the population, interstate relations and even military interests, traditionally part of national security, now used to also define public security, demonstrate how blurred the boundaries between these two concepts of security have come to be. Adding to that, combatting terrorism expressly falls within the scope of both national and public security.[26]

In the CJEU's view, 'a threat to national security must be *genuine and present, or at the very least foreseeable*' and is thereby 'distinguishable by its *nature, its 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 offences

[22] A Dimitrova and M Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2018) 56 Journal of Common Market Studies 751, 760; Vogiatzoglou and Fantin (n 7).

[23] Case C-145/09 *Land Baden-Württenberg v Panagiotis Tsakouridis* EU:C:2010:708 para 44 and case law cited therein.

[24] The recital continues by repeating the case law as follows: 'a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests'. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, recital 19. See also Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, recital 12, according to which a threat to public security may further include 'a particularly serious threat to one of the fundamental interests of society'.

[25] Art 83(1) TFEU. See also Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970 para 103.

[26] See for example *Tele2 Sverige* (n 25) para 103; *La Quadrature du Net* (n 4) para 135.

being committed'.[27] Nevertheless, the nature and seriousness of threats against national and public security are similarly defined as genuine and as relating to the same fundamental state and society interests, as discussed above. Ultimately, the determining factor may be temporal, as the threat to national security is present or foreseeable, whereas a threat to public security is seen as general and permanent.[28] Yet, in such a dynamic and complex environment like security, distinguishing between *foreseeable* and *general* may not be as explicit either.[29] Furthermore, the guidance by the CJEU seems to neglect the growing collaboration and institutional blurred lines between intelligence services, competent for national security, and law enforcement authorities, competent for public security, for example, working together to prevent terrorist acts.[30] Adding to that complexity, private sector actors are increasingly involved in security activities, with a crucial impact in delineating the scope of EU competences and data protection law.

2.2. Private sector and the expanding application of EU law

As with every exception to EU law, the national security derogation under Article 4(2) TEU must be interpreted strictly. The CJEU has consistently held that Member States are not allowed to unilaterally decide to completely override EU obligations for purposes of national security unless they have sufficiently substantiated their claim.[31] A derogation from an EU obligation cannot take place in the abstract, but the Member State in question must demonstrate specifically and 'to the requisite legal standard' that the derogation is necessary. In this way, the Court does not

[27] *La Quadrature du Net and Others* (n 4) paras 136–137. Case C-140/20 *Commissioner of An Garda Síochána* xEU:C:2022:258 para 62.

[28] Ibid.

[29] M Tzanou and S Karyda, 'Privacy International and Quadrature Du Net: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28 *European Public Law* 123, 137–138; V Mitsilegas, E Guild, E Mendos Kuşkonmaz and N Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2022) 29 *European Law Journal* 176, 197; P Vogiatzoglou, 'Case note on the Court of Justice C-140/20 Commissioner of An Garda Síochána ruling' (2022) *Computerrecht* 272, 277.

[30] See *inter alia* C Cocq and F Galli, 'The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes' (2013) 4 *New Journal of European Criminal Law* 256; A Završnik, 'Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?' (2013) 9 *Journal of Contemporary European Research* 181.

[31] Case C-300/11 *ZZ v Secretary of State for the Home Department* EU:C:2013:363 para 38; Case C-808/18 *European Commission v Hungary* EU:C:2020:1029 para 261; Case C-715/17, C-718/17 and C-719/17 *European Commission v Republic of Poland and Others* EU:C:2020:257 para 143; *La Quadrature du Net and Others* (n 4) para 99. See also M Claes, 'The Primacy of EU Law in European and National Law' in D Chalmers and A Arnull (eds), *The Oxford Handbook of European Union Law* (Oxford University Press 2015) 178.

unconditionally accept the invocation of Article 4(2) TEU by Member States, but instead examines whether EU law may still be applicable in the case at hand.

Accordingly, in its now (in)famous *Privacy International* and *LQdN* judgments, the CJEU conditioned the national security derogation upon the lack of private actors. In particular, the rulings clarified that the national security exception is applicable only when it concerns practices that are purely governmental, this means that they do not engage any private entity subject to EU rules.[32]

To reach this conclusion, the CJEU built not only on its settled case law that 'the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable',[33] but also on its rich data retention jurisprudence. In fact, the activities of private entities have been playing a determinant role in defining the scope of EU law applicability, already since the litigation regarding the legal basis of the now invalidated Data Retention Directive (DRD).[34] In turn, a series of cases regarding the e-Privacy Directive (EPD),[35] and its Article 15(1), which allows the adoption of national data retention measures for national and public security purposes, helped shape the court's argumentation. Interestingly enough, its line of reasoning, especially as regards the scope of ECSPs activities, has not been entirely consistent throughout time.

More specifically, when deciding on the fate of the DRD legal basis, the Court held that, since the DRD governed only the *retention* of electronic communications services (ECS) metadata[36] by private entities, and *not their subsequent access* and use, it did not concern law enforcement purposes or any state activities.[37] In fact, the Court found data retention as such to be of commercial nature, independent of any security activity.[38] The role of the private sector served in this case as a means to

[32] *Privacy International* (n 4) para 49; *La Quadrature du Net and Others* (n 4) paras 103-104. See also Case C-101/01 *Criminal proceedings against bodil Lindqvist* EU:C:2003:596 para 43 and Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* EU:C:2008:54 para 51.

[33] Ibid.

[34] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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.

[35] Directive on privacy and electronic communications (n 15).

[36] Metadata in the context electronic communications services refer to traffic and location data. Traffic data are defined as 'data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof' and location data are defined as 'data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'. Directive on privacy and electronic communications (n 15) Art 2(b) and (c) respectively.

[37] C-301/06 *Ireland v European Parliament and Council of the European Union* EU:C:2009:68 paras 80, 91.

[38] Ibid paras 82–83.

confirm the DRD legal basis of the EU internal market, rather than the then third pillar where the EU enjoyed less power.[39] By contrast, in *Tele2* a few years later, the CJEU held that the data *retention* by ECSPs and the *access* to the retained data by security authorities fall within the scope of the EPD.[40] This approach seems to have come as a response to Member States and the Commission claiming that only national legislation relating to data *retention* must abide by the EPD;[41] the Court stated clearly that also data access comes within this scope.

To that end, the CJEU took into account the general structure of the EPD, which applies to ECSPs, and its Article 15(1), which foresees the adoption of national data retention schemes derogating from EPD obligations.[42] Still, Article 15(1) EPD, in the same way as the invalidated DRD, does not refer to *access* to the retained data. Nevertheless, the CJEU stated that data are retained 'only for the purpose, when necessary, of making that data accessible to the competent authorities'.[43] The fact that data are retained for the sole purpose of being accessed to by security authorities had been previously neglected.[44] Moreover, in a rather conflicting way, the Court admitted that 'the legislative measures that are referred to in [art. 15(1) EPD] concern *activities characteristic of States or State authorities, and are unrelated to fields in which individuals are active*'.[45] Without bringing forth any counter-argument, the CJEU posited, however, that Aricle 15(1) EPD 'expressly authorises' such legislative measures, and thus they necessarily fall within its scope.[46] Any different

[39] Ibid para 93 with reference to Treaty of Nice [2001].

[40] *Tele2 Sverige* (n 25) paras 78 and 82.

[41] Ibid paras 65–66.

[42] In particular, according to Directive on privacy and electronic communications (n 15), Art 15(1), 'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in [..] this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC'. See also *Tele2 Sverige* (n 25) para 73.

[43] *Tele2 Sverige* (n 25) para 79.

[44] The CJEU had in fact been subject to criticism for its DRD ruling, disregarding how retention and access are inextricably connected, see F Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-Level* (Springer 2012) 392–393.

[45] The Court even admitted that the objectives pursued by such measures substantially overlap with the objectives that fall outside the scope of the Directive on privacy and electronic communications (n 15) as per its art 1(3). *Tele2 Sverige* (n 25) para 72.

[46] *Tele2 Sverige* (n 25) para 73.

conclusion, in the court's debatable view,[47] would deprive the provision under Article 15(1) EPD of any purpose.[48]

Throughout its argumentation, the Court did not touch upon how different security purposes may be pursued by national data retention measures in line with Article 15(1) EPD. In fact, Advocate General (AG) Øe interpreted the *Tele2* ruling as bringing 'national provisions, based on [art. 15(1) EPD] governing both the retention by [ECSPs of metadata], as well as the access by the public authorities to the data retained for the purposes referred to in that provision – *which include* law enforcement *and the protection of national security* – [..] *within the scope of that directive*'.[49] In this way, the outcome in *Privacy International* and *LQdN* extending the EPD scope to national security activities should not come as a surprise.

In the meantime, another building block was added with *Ministerio Fiscal*, whereby the CJEU clarified that the Article 1(2) EPD excludes from its scope activities of the state that 'are unrelated to field in which individuals are active' – the phrase previously used to describe the national measures adopted pursuant to Article 15(1) EPD.[50] Conversely, national measures imposing retention of data and access to retained data fall within the scope of the EPD, and are governed by Article 15(1) EPD. Through this rather circular argumentation, it was asserted that these national measures regulate activities of ECSPs, and 'cannot be regarded as activities characteristic of States'.[51] In *Tele2* and *Ministerio Fiscal*, the central role of the private sector actors[52] allowed the extension of EU rules applicability, by shifting the scope of their activities to also encompass the access to retained data. However, it should be noted that these cases concerned processing activities for the purpose of public security, where the EU enjoys clear regulating powers.

Finally, in *Privacy International* and *LQdN*, the scope of ECSPs activities allowed the CJEU to confirm that national data retention legislation at large falls within the scope of the EPD.[53] Based on *Tele2* and *Ministerio Fiscal*, the Court affirmed how '[such] legislative measures *necessarily involve the processing, by [ECSPs]*, of the data and *cannot* [..] *be regarded as activities characteristic of States*'. Therefore, the entire data retention framework, comprised of the processing activities of both the retention by ECSPs and the granting of access to security authorities, for both national

[47] See *inter alia* I Cameron, 'Metadata Retention and National Security: Privacy International and La Quadrature Du Net' (2021) 58 *Common Market Law Review* 1433, 1458.

[48] Ibid.

[49] Opinion of AG Øe in Case C-311/18 *Data Protectioin Commissioner v Facebook Ireland Limited and Maximillian Schrems* EU:C:2020:559 para 215.

[50] Case C-207/16 *Proceedings brought by Ministerio Fiscal* EU:C:2018:788 para 32.

[51] Ibid para 37.

[52] See also Mitsilegas, Guild, Mendos Kuşkonmaz and Vavoula (n 29) 5.

[53] *Privacy International* (n 4) paras 34–39; *La Quadrature du Net and Others* (n 4) paras 91–103.

and public security, is subject to and must comply with the EPD.[54] By consequence, it must also comply with the General Data Protection Regulation (GDPR), which is supplemented and specified by the EPD.[55] To reinforce its argumentation, the CJEU further claimed that the GDPR, too, foresees exceptions from the application of certain of its provisions for security purposes, and thereby, '*it is apparent from Article 23(1)(d) and (h) [GDPR] that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation'*.[56]

To sum up, the conclusion that arises from the CJEU's data retention case law is that EU rules are applicable to national measures which impose obligations upon private sector actors, whose activities are regulated by EU law, such as ECSPs. Therefore, these national measures – even if they are pursuing the safeguarding of national security – are subject to CJEU scrutiny. By extending the applicability of EU law to activities even in pursuit of national security purposes, it brought them under the safeguards of EU data protection law, as well as the Charter.[57] However, the Court took a questionable route to reach this conclusion, and its reasoning is far from robust or well-substantiated, to say the least.[58] The incoherent building of argumentation on what constitutes activities of states, the unique understanding of what foreseeing an exception entails and the limited analysis of the Article 4(2) national exclusivity on national security matters have failed to convince Member States of the judicial interpretation of the scope of EU law applicability (see below Section 3). As a result, this case law is liable to result in more fragmentation rather than establishing clear boundaries between national and public security activities. Furthermore, drawing a distinction between ECSPs activities broadly understood, and purely state activities narrowly understood, may not be as easy to operationalise in practice either, as security tasks more often than not rely on the private entities which have taken over critical infrastructures such as ECS.[59]

[54] *Privacy International* (n 4) paras 46–47; *La Quadrature du Net and Others* (n 4) paras 101–102.

[55] 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-GDPR), Art 95. See also ibid.

[56] *Privacy International* (n 4) para. 47; *La Quadrature du Net and Others* (n 4) para 102.

[57] Nevertheless, expanding EU law applicability to national security activities has a sword function as well, since it brought mass surveillance into its scope. More specifically, according to the CJEU, mass, that is, general and indiscriminate surveillance, is permitted for purposes of national security, while the objective of public security may only justify surveillance which is targeted, that is restricted in relation to categories of persons or data concerned. *La Quadrature du Net and Others* (n 4) paras 137 and 147 respectively.

[58] See also critiques raised by Cameron (n 47); Tzanou and Karyda (n 29); Mitsilegas, Guild, Mendos Kuşkonmaz and Vavoula (n 29).

[59] Cameron (n 47) 1458–1459.

3. The legal uncertainty arising from the current delineation of the scope of EU data protection law

3.1. Narrowing the scope back down? The draft E-Privacy Regulation and the AI Act

Member States in general, and France in particular, were dissatisfied, to say the least, with the expansive approach by the CJEU.[60] In this vein, the Council position adopted in the context of the negotiations for the draft E-Privacy Regulation (which would replace the EPD),[61] introduced several provisions that essentially seek to circumvent the above jurisprudence.[62] Specifically in relation to national security, the Council inserted a clause excluding from the scope of the draft E-Privacy Regulation: 'measures, processing activities and operations concerning national security and defence, *regardless of who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority*'.[63]

Most likely prompted by the CJEU's expansive interpretation of the scope of the EPD, a similar exclusion clause was introduced to the Proposed AI Act by the Council.[64] Following fierce negotiations and the unyieldingness of certain Member States led by France, the national security exemption made it to the final text of the AI Act.[65] Accordingly, the AI Act

[60] As reported in media, see for example T Christakis and K Propp, 'How Europe's Intelligence Services Aim to Avoid the EU's Highest Court – and What It Means for the United States' (Lawfare Blog, 8 March 2021), at www.lawfareblog.com.

[61] Proposal for a Regulation of the European Parliament and of the Council of 10 January 2017 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 – Proposal for E-privacy Regulation) COM(2017) 10 final - 2017/03 (COD). The E-Privacy Regulation was eventually withdrawn in February 2025, under the justification of 'no unforseeabble agreement' between the co-legislators. Civil society has raised the concern that the proposal was blocked by not only Big Tech companies, but also member states that seek to ensure bbroader surveillance powers. Annexes to the Communitcation from the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission work programme 2025 of 11 February 2025, 27; EDRi, 'The ePrivacy Regulation Proposal has been withdrawn, but the figh for your privacy is far from over' (EDRi, 19 February 2025), at edri.org.

[62] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council of 10 February 2021 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) – Mandate for negotiations with EP, 6087/21.

[63] Ibid Art 2(a).

[64] Council of the European Union Presidency, Proposal for a Regulation of the European Parliament and of the Council of 25 November 2022 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach, 14954/22, Art 2(3).

[65] Besides, the national security exception phrased in that way was already established in the Data Act. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023

> 'does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.
> This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.
> This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities'.[66]

As further explained in the recitals, the exclusion is justified by Article 4(2) TEU appointing sole responsibility of national security matters upon Member States.[67] Where the AI system is placed on the market or put into service for both national and public security purposes, though, it must still abide by the AI Act.

Both these pieces of secondary legislation are crucial in regulating surveillance practices given the strong reliance on ECS data as well as the proliferation of advanced technologies promising to facilitate the fight against crime and the safeguarding of security.

That being said, the legitimacy of the European legislator challenging the European judiciary's rulings raises significant concerns. Indeed, if the final adopted texts maintain a derogation from the scope of relevant EU secondary laws of any national security activity regardless of the undertaking actor, will that entail a complete abolition of the CJEU red lines?

First, as pointed out by the European Data Protection Board (EDPB), the proposed exclusion in the E-Privacy Regulation risks fragmenting the consistency of the EU data protection framework, while in any case, the GDPR continues to apply.[68] In other words, this clause only excludes the applicability of the E-Privacy Regulation, which acts as *lex specialis* in relation to the GDPR;[69] the latter is meant to regulate all data processing activities by entities, including ECSPs, insofar as other specific laws, such as the EPD, do not provide for different rules.[70] This point was to an

on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, Art 1(6).

[66] Art 2(3) AI Act.

[67] Recital 24 AI Act.

[68] European Data Protection Board, Statement 03/2021 on the ePrivacy Regulation (9 March 2021).

[69] Recital 173 GDPR.

[70] See also M Rojszczak, 'The Uncertain Future of Data Retention Laws in the EU: Is a Legislative Reset Possible?' (2021) 41 *Computer Law & Security Review*, 9.

extent implied by the CJEU in *LQdN*;[71] although only referring to the national security derogation within Article 23 GDPR, the statement was put forward by the CJEU to solidify its argumentation on how individuals acting in the scope of these derogations are still subject to the GDPR.

Second, as demonstrated above, the CJEU has in essence defined the ECSPs' operations as activities that are not characteristic of the state. It may therefore be questioned to what extent activities 'concerning national security and defence' can, in fact, be interpreted as encompassing the ECSPs' activities, as the Council suggests.[72] A study for the European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware' (hereinafter 'PEGA Committee') has similarly submitted that the assessment of the nature of state activities necessarily pertains to EU law and is subject to CJEU scrutiny.[73] In this way, the last say regarding what constitutes an ECSPs' activity is with the CJEU. If – or, most likely, when – the CJEU is confronted with this exclusion provision, an equally expansive applicability of EU (data protection) law could arguably be adopted.[74]

Finally, it may be claimed that the CJEU jurisprudence is primarily rooted in the Charter and the rights to privacy and to personal data protection enshrined therein,[75] and as such, must be upheld insofar as the Charter applies. Member States must comply with the Charter both when implementing EU law into their national legal order, and when derogating from EU law as foreseen in the EU Treaties.[76] The CJEU has even found rights such as the right to an effective remedy under Article 47 and the right to non-discrimination under Article 21 Charter to apply also in horizontal relations between private entities,[77] while the possible horizontal effect of the right to personal data protection under Article 8 Charter has also been explored.[78] This brings the issue back to Article 4(2) TEU, as the Charter does not apply when Member

[71] *Privacy International* (n 4) para. 47; *La Quadrature du Net and Others* (n 4) para 102.

[72] Rojszczak (n 70).

[73] Sartor and Loreggia (n 8) 47.

[74] See also ibid.

[75] Council of the European Union, 'Informal Outcome of Proceedings of the informal VTC of the members of CATS on 8 February 2021' (26 February 2021), WK 2732/2021 INIT, at cdn.netzpolitik.org 4.

[76] Art 51(1) of the Charter of Fundamental Rights of the European Union [2012]. See *inter alia* Case C-260/89 *Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdelias and others* EU:C:1991:254 para 43; Case C-617/10 *Åkiagaren v Hans Akerberg Fransson* EU:C:2013:105 paras 17–21.

[77] Case C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.* EU:C:2018:257 paras 59, 82. See also K Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 *German Law Journal* 779, 788.

[78] See for example M Tzanou, 'The Unexpected Consequences of the EU Right to Be Forgotten: Internet Search Engines as Fundamental Rights Adjudicators' in M Tzanou (ed) *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020) 279.

States act outside the scope of EU law; however, as aforementioned, the invocation of Article 4(2) TEU to derogate from EU law has been interpreted very restrictively. In that regard, diverse opinions have been expressed; Kosta considers that the lack of reference to the Charter in the discussion on the scope of EU law implies that in cases of national security, the Charter does not apply pursuant to Article 4(2) TEU.[79] By contrast, Rojszczak puts forth that the judicial interpretation of what constitutes proportionate limitations to the rights to privacy and to data protection on the basis of the Charter remains unaffected.[80] Building on previous CJEU rulings on Article 4(2) TEU,[81] Hijmans has also argued that general EU standards on fundamental rights, including the data protection regime based on Article 16 TFEU, 'could, in principle, be applied to national security agencies'.[82] As a derogation from EU law must be strictly interpreted and sufficiently substantiated, even in cases of national security, it is hereby argued that derogating from respecting the right to personal data protection in line with the Charter cannot be unilaterally decided by Member States.

3.2. National security and new forms of surveillance

There are other crucial forms of private entities' involvement in national security processing that go beyond data retention by ECSPs and concern automated processing or other forms of surveillance. To illustrate the legal uncertainties surrounding the grounding of the applicability of EU law for national security processing operations on the activities of private entities, such as ECSPs, we make use of two case studies.

The first case study arises from a recent judgment, where the German Federal Constitutional Court found that the use of the Palantir software[83] by police in Hesse and Hamburg was unconstitutional.[84] Palantir was used as a data analysis instrument with the purposes of averting terrorist threats and combatting organised crime.[85] It undertook automated data analysis aimed at generating new knowledge, by establishing connections between people, groups of people, institutions, organisations, objects and things, excluding insignificant information and findings, assigning

[79] E Kosta, 'A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon' in E Kosta, R Leenes, and I Kamara (eds) *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 68, 86. See also Korff (n 9).

[80] Rojszczak (n 70) 10. See also Sartor and Loreggia (n 8).

[81] *ZZ* (n 31), reference to which is made in *La Quadrature du Net and Others* (n 4) para 99.

[82] H Hijmans, *The European Union as a Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer 2016) 142–143.

[83] See *inter alia* D Howden, A Fotiadis, L Stavinoha and B Holst, 'Seeing Stones: Pandemic Reveals Palantir's Troubling Reach in Europe' (The Guardian, 2 April 2021), at www.theguardian.com.

[84] 1 BvR 1547/19 and 1 BvR 2634/20, judgment of 16 February 2023.

[85] Ibid.

incoming information to known facts and the statistical evaluation of the stored data.[86] It allowed the public authorities to skim far-reaching knowledge from the available data with practically all possible information technology methods and develop new connections from the evaluation.[87] This linking of data allowed, among others, multi-stage analyses that first generate new suspicions, as well as further analysis steps or subsequent operational measures.[88]

In this case, Palantir was used by the police for law enforcement purposes and, thus, would come within the scope of the Law Enforcement Directive (LED),[89] which, surprisingly, the Federal Constitutional Court did not mention in its judgment. However, let us assume for a moment that a similar commercially developed AI software is used by intelligence services for national security purposes. Following the CJEU data retention line of cases, it is unclear whether such processing would fall in or outside the scope of application of EU law, because the involvement of private entities here concerns the *automated processing* of ECS data by state securities through a software developed by a private entity not subject to EU law. In this vein, a narrow reading of the CJEU's data retention cases focusing on ECSPs would exclude such processing from the scope of EU law.

However, a broader reading of these cases, recently proposed by certain scholars would bring such processing within the application of EU law. For instance, Korff has argued that even where AI systems are deployed by national security agencies alone, thereby comprising purely governmental activities, applicability of EU law may still be invoked by virtue of their collaboration with entities subject to EU law.[90] Indeed, intelligence services rarely function in a vacuum but instead share data with, amongst others, national law enforcement or other specialised security authorities, subject to the LED or EU agencies such as Europol. This is certainly supported by the Palantir example, where in the German State of Hesse, Palantir had access to mainly three databases POLAS (police information system for 'repressive' data), ComVor (case processing system for all procedures) and CRIME-ST (case processing system for storing 'preventive' data for future investigations);[91] but also used further data sources, including – among others – 'traffic data from telecommunications monitoring' provided by telecommunications providers. While a broad reading of the CJEU's data retention jurisprudence is possible here, such approach is to say the least debatable.

[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Directive (EU) 2016/680 (n 24).
[90] Korff (n 9).
[91] HessLT Drucks 20/660, 2

Let us now consider a second case study. Imagine that an EU Member State uses against EU citizens for counter-terrorism and national security purposes, a modern spyware tool, such as Pegasus, developed and marketed by a private company (in this case, the Israeli NSO Group).[92] Pegasus is considered 'the most powerful hacking tool or spyware'[93] to date, because it grants 'complete, unrestricted access' to the targeted mobile phone device, its sensors and all the information contained on this (including geolocation).[94] This means that it can read end-to-end encrypted messages, download stored photos, hear voice/video calls and activate the phone's microphone and camera to record conversations.[95] Alarmingly, all this can be carried out through a so-called 'zero-click' attack; this means that even the most tech-savvy users would not be aware of the attack as it does not require any action by the user to be tiggered.[96] Finally, the Pegasus software is 'very difficult to detect' and its 'intrusions are very hard to prove', making it a 'game-changer for digital surveillance'.[97]

Pegasus is developed and deployed by a private company but procured and used by national security agencies. It entails targeted surveillance that differs from the bulk data retention model, seen in *Privacy International* and *LQdN*. Such a processing would also fall outside the scope of EU law because the involvement of private operators does not implicate an ECSP or another entity subject to EU law.[98] Yet, Pegasus' level of intrusiveness is 'unprecedented'.[99] Indeed, as the EDPS rightly noted, the use of Pegasus 'threatens the *essence of the right to privacy*, as the spyware is able to interfere with the most intimate aspects of our daily lives'.[100] Conversely, the European Parliament 'Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware' attempted in its Recommendation to the Council and the Commission to bring within the scope of the EPD the use of spyware, such as Pegasus, arguing that the deployment of such surveillance tools by Member

[92] This is not just a hypothetical situation as 'some EU governments admitted to having bought Pegasus', and it has been reported that the Pegasus spyware has been 'used in the EU against EU citizens, including opposition politicians, journalists and lawyers'. European Data Protection Supervisor (n 1) 6; 'Hungary Admits to Using Pegasus Spyware' (Deutsche Welle, 11 April 2021) at www.dw.com; Z Wanat, 'Poland's Watergate: Ruling Party Leader Admits Country has Pegasus Hacking Software' (Politico, 7 January 2022), at www.politico.eu.

[93] European Data Protection Supervisor (n 1) 3.

[94] Pegg and Cutler (n 2).

[95] European Data Protection Supervisor (n 1) 3.

[96] Ibid.

[97] Ibid.

[98] A contrario see Sartor and Loreggia (n 8) noting that 'We submit that this preliminary issue, pertaining to the qualification of nature of the state activities, necessarily pertains to EU law, and therefore falls within the competence of the ECJ'.

[99] European Data Protection Supervisor (n 1) 2.

[100] Ibid.

States 'constitutes a restriction of the right to protection of terminal equipment afforded by the e-Privacy Directive'.[101] While it is welcome that the EP PEGA Committee would like to find an interpretation of the EPD which brings the deployment of spyware within the scope of EU fundamental rights law, the mention of 'a right to protection of terminal equipment' under the EPD is confusing: what is the content of such right and what obligations does it create? More importantly, it appears to offer another means to circumvent the overall problem of the applicability of EU data protection law to modern surveillance tools; this has to be grounded once again on -uncertain- provisions of the EPD.

3.3. Grounding the EU law applicability on secondary law interpretations

The examined case studies demonstrate that the centring of the applicability of EU law in national security matters on interpretations of the EPD and the role of ECSPs is problematic and short-sighted. First, as discussed in Section 2, it is problematic, because it relies on an artificial distinction of what constitutes private and public functions that is unworkable in practice, where the traditional model of data retention by private actors and access and further processing by public authorities is often blurred. The increasing responsibilisation of the private sector in performing security tasks on behalf of the state will only blend these boundaries more.[102] Additionally, the CJEU has confusingly expanded the scope of what constitutes an ECSP activity, from *retention* to *access* to 'all operations processing personal data carried out' by ECSPs,[103] by interpreting broadly the exclusion and restriction clauses within the EPD and the GDPR, while at the same time interpreting narrowly Article 4(2) TEU. In this way, this approach depends on the interpretation of derogations within primary and secondary law, which, is perpetually found in a tag war, with the CJEU pulling more and more towards the realm of EU law, and the Member States demanding their unrestricted freedom in matters of national security. Consequently, reliance on the actor/controller to determine the applicability of EU (data protection) law in matters of national security results in increased legal uncertainty.

Second, this approach is short-sighted, because, while it relies on a teleological interpretation of existing data protection instruments, such as the EPD, it misses out on two fundamental aspects of EU data protection law: On the one hand, it fails to account for other crucial forms of private entities' involvement in personal data processing for national security purposes. While it captures communications' data

[101] PEGA Committee, Recital AF.

[102] The responisibilisation strategy was first introduced by D Garland, 'The Limits of the Sovereign State - Strategies of Crime Control in Contemporary Society'(1996) 36 *The British Journal of Criminology* 445. See further contributions within this issue.

[103] *La Quadrature du Net and Others* (n 4) para 101.

retention by ESPs, it leaves untouched potential data processing undertaken by intelligence agencies with different ways of involvement of private entities, which entail for instance, the public procurement of data mining and analysis software, such as the one developed by Palantir, or indeed spyware software, such as Pegasus. On the other hand, by regrettably excluding from the scope of application of EU data protection law surveillance tools that encroach on the very essence of the fundamental rights to privacy and data protection, it falls short from achieving the overarching fundamental goals of EU data privacy law that are to protect both individual data subjects from such invasive (new forms of) surveillance and to ensure 'the functioning of democracy'[104] and the rule of law, 'since privacy is a core value inherent to a liberal democratic and pluralist society'.[105]

Against this background, we argue that there is an urgent need to *rethink* the current grounding of the scope of applicability of EU data protection law on processing activities in the context of electronic communications. While the CJEU's data retention jurisprudence is welcome because it clearly demonstrates that the area of national security is not outside the purview of EU fundamental rights, it is no longer fit for purpose to address the 'corporate and government entanglements'[106] regarding the collection and processing of personal data and new forms of intrusive surveillance. The following Section situates our proposed model in the conceptual framework of digital constitutionalism and draws inspiration from the theoretical debates surrounding this framework to develop a comprehensive theory underpinning the proposed approach.

4. Rethinking the scope of application of EU law in the context of national security: a new approach

4.1. National security through the prism of digital constitutionalism

Digital constitutionalism is a theoretical framework that adapts the values and ideals which permeate, inform and guide the process of constitutionalisation to the digital environment.[107] As a relatively new theoretical (and practical) field of

[104] European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (FRA, 27 November 2019) at fra.europa.eu 4 and 28.

[105] Ibid. 4 and 28. For a detailed analysis, see below.

[106] A Campolo, M Sanfilippo, M Whittaker, K Crawford, 'AI Now 2017 Report' ainowinstitute.org

[107] E Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 *International Review of Law, Computers & Technology* 76. See *inter alia* V Karavas, 'Governance of Virtual Worlds and the Quest for a Digital Constitution' in C Graber and M Burri-Nenova (eds) *Governance of Digital Game Environments and Cultural Diversity: Transdisciplinary Enquiries* (Edward Elgar Publishing

constitutionalism, digital constitutionalism focuses on how digital technologies affect the evolution of constitutionalism by investigating the dynamic dialectic between the 'digital' and 'constitutionalism'.[108] The 'digital' refers to the Internet and automated technologies, while 'constitutionalism' denotes the basic idea of constitutional law that power (of governments) should be legally limited and the legitimacy of such power is dependent upon compliance with those limitations.[109] Digital constitutionalism, thus, aims to explore 'the reaction of constitutional law against the power emerging from digital technologies implemented by public and private actors'[110] and to articulate the limits to the exercise of such power in the digital society. The digital constitutionalism literature, despite being fairly recent, has various iterations with certain authors focusing on its ability to constrain private power and private actors in the digital space,[111] others looking at public power and the role of national governments[112] and a further strand proposing the creation of new 'digital' bills of rights.[113]

Overall, digital constitutionalism offers a framework 'to rethink how the exercise of power ought to be limited (made legitimate) in the digital age'.[114] As Suzor notes eloquently, 'digital constitutionalism requires us to develop new ways of limiting

2010) 153; K Milewicz, 'Emerging Patterns of Global Constitutionalisation: Towards a Conceptual Framework' (2009) 16 *Indiana Journal of Global Legal Studies* 413; C Padovani and M Santaniello, 'Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System' (2018) 80 *International Communication Gazette* 295; I Pernice, 'Global Constitutionalism and the Internet. Taking People Seriously' in S Kadelbach and R Hofmann (eds), *Law Beyond the State: Pasts and Futures* (Campus Verlag 2016) 151; A Simoncini, 'The Constitutional Dimension of the Internet: Some Research Paths' (EUI Working Papers 16-2016); G Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford University Press 2012); JHH Weiler and M Wind (eds), *European Constitutionalism Beyond the State* (Cambridge University Press 2003); KM Yilma, 'Digital Privacy and Virtues of Multilateral Digital Constitutionalism—Preliminary Thoughts' (2017) 25 *International Journal of Law and Information Technology* 115.

[108] G De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19 *International Journal of Constitutionsl Law* 41, 58.

[109] Ibid.

[110] Ibid.

[111] B Fitzgerald, 'Software as Discourse? A Constitutionalism for Information Society' (1999) 24 *Alternative Law Journal* 144; N Suzor, 'The Responsibilities of Platforms: A New Constitutionalism to Promote the Legitimacy of Decentralized Governance' (Association of Internet Researchers Annual Conference, 2016).

[112] Celeste (n 107).

[113] J Zittrain, 'A Bill of Rights for the Facebook Nation' (The Chronicle of Higher Education, 20 April 2009) at www.chronicle.com; D Redeker, L Gill and U Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2018) 80 *International Communication Gazette* 302.

[114] N Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4 *Social Media+Society* 1.

abuses of power in a complex system that includes many different governments, businesses, and civil society organizations'.[115]

We adopt digital constitutionalism as a theoretical framework for the purposes of the present analysis; our aim is to rethink how the exercise of national security surveillance powers ought to be limited in the European digital environment. The ultimate goal of this rethinking is to develop new ways of limiting abuses of power in this context. This rethinking focuses on two basic aspects of digital constitutionalism (and constitutional law in general): *i)* the protection of fundamental rights, and *ii)* the balancing of powers.[116] We use digital constitutionalism as a conceptual prism for our discussion because modern surveillance technologies, such as Palantir and Pegasus affect the protection of fundamental rights -and in particular the right to data protection- in the digital space. However, we understand the balancing of powers slightly differently from traditional constitutional law articulations here: these concern the vertical distribution of powers (between the EU and its Member States). Therein, an added layer of complexity derives from national security as a limitation between EU and Member State powers. How does this balancing of powers between the EU and its Member States affect fundamental rights protection in the digital society when national security measures are at stake? In light of the risks that are exacerbated in the digital domain, how could we develop new ways of limiting abuses?

In our view, both these questions should be analysed within the framework of EU digital constitutionalism and with the tools offered by it, as the exercise of national security powers impacts the fundamental rights of EU citizens. Our primary focus is on the protection of fundamental rights, while the involvement of both private entities and national security operations are important parameters to our analytical framework.

For the purposes of this discussion, digital constitutionalism is understood as providing the imperative that underpins the process of constitutionalisation, offering, in this way, the production of different 'normative counteractions that address the challenges of digital technology'.[117] We view constitutionalisation as a dynamic process comprising different stages,[118] rather than referring only to the final outcome of a process in which norms are institutionalised or constitutionalised.[119] We, therefore,

[115] N Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019).

[116] A Peters, 'Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures' (2006) 19 *Leiden Journal of International Law* 579.

[117] Celeste (n 107) 77.

[118] Ibid; E Celeste, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2018) 33 *International Review of Law, Computers & Technology* 1.

[119] Ibid.

subscribe to an understanding of constitutionalisation, which considers that the development of constitutional principles at the societal level can mark the presence of a process of constitutionalisation in the digital environment, even if norms are not yet institutionalised or positivised in the hierarchy of legal sources.[120] Lastly, we see this dynamic process of constitutionalisation of the digital environment as not unitary[121] and involving not only formal, institutionalised actors, such as courts or legislators, but also other voices, such as civil society and academia.

The *data subject* model developed and proposed in this article is our new way of limiting abuses of power in the EU legal order when national security practices in the digital domain affect individuals. This model is developed as a normative counteraction to address the challenges of different forms of surveillance used for the purposes of national security and the legal uncertainty of current regulatory and judicial attempts. Its ultimate aim is to achieve 'constitutional equilibrium', broadly understood as 'the ideal condition produced by the application of the norms of constitutional law in a given legal order'.[122] We consider the applicability of EU fundamental rights to national security measures as a pre-condition for the achievement of the constitutional equilibrium in this area, without which the substantive fundamental rights protection cannot be realised.

We argue that a process of (digital) constitutionalisation has already commenced in the area of data retention, with the CJEU leading this. However, in our view, the Court's normative counteraction in this context is no longer sufficient or fit for purpose.[123] We, therefore, see our new approach as advancing the dynamic process of this constitutionalisation while addressing the limitations of the Court's data retention jurisprudence.

4.2. A new *data subject-centric* model

A first way of delimiting the scope of application of EU law in the context of national security is based on the *purposes of processing* (we call this the *purposes model*). According to the purposes model, which has been proposed by Member States, if data processing is undertaken for national security purposes, it falls automatically outside the scope of EU law pursuant to Article 4(2) TEU. The purposes model has been rightly rejected[124] – at least partially – by the CJEU in favour of a different

[120] Karavas (n 107); Celeste (n 107).

[121] Celeste (n 107); A Peters, 'Global Constitutionalism' in M Gibbons (ed), *The Encyclopedia of Political Thought* (John Wiley & Sons 2014).

[122] Celeste (n 118).

[123] See discussion above.

[124] We consider that this is right, because Member States tend to often invoke the national security exception to escape EU law obligations.

approach, which grounds the scope of applicability of EU law, in the context of national security, on the activities of ECSPs. While the purposes underlying the processing operations are important in order to determine the level of intrusiveness that may be justifiable in terms of bulk or targeted surveillance,[125] since such activities are regulated by the EPD, data retention falls within the scope of EU law in cases where ECSPs are compelled by national security agencies to carry out processing activities for national security purposes. We call this the *controller model* as the applicability of EU law is based on the regulation of the activities of *data controllers* (here the ECSPs).

Under the framework of digital constitutionalism, this article proposes a novel, third model of establishing the scope of applicability of EU law that should be grounded on the *data subject* instead (we call this the *data subject model*). The data subject model envisions the applicability of EU law to national security measures where these involve the monitoring of the behaviour or the processing of personal data of data subjects within the EU. This would mean that EU law would be applicable in both case studies discussed above as all of them concern the monitoring of the behaviour/ processing of personal data of EU data subjects.

Privacy scholars, such as Korff, have called for national security agencies to be made subject to EU law and the Charter.[126] Their arguments are normally based on the Court's expansive data retention case law discussed above. However, the data subject model, proposed here, differs from Korff's for two reasons. First, we call for a general shift from the focus on controllers to data subjects when establishing the applicability of EU law in the national security context. Second, we argue that there is a theoretically and doctrinally more robust framework to achieve this, which differs from what has already been proposed. This is, therefore, a novel approach that attempts to move forward from what has been established in the case law and argued in the academic legal scholarship.

Nevertheless, we submit that *data subject model* is not radical or unfeasible from a legal point of view. Indeed, it is inspired by current and proposed legislative frameworks as both the GDPR and the AI Act adopt a data subject approach when considering questions of the territorial application of the relevant law. Article 3(2) GDPR establishes the *ratione loci* of this Regulation: *'to the processing of personal data of data subjects who are in the Union* by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or

[125] See Section 2.

[126] Korff has suggested that 'entities that, while established in the EU, are not subject to EU law or the Charter – i.e., to the EU Member States' national security agencies' should be subject to EU law. See Korff (n 9).

services,…to such data subjects in the Union; or (b) *the monitoring of their behaviour as far as their behaviour takes place within the Union*'.[127]
Along the same lines, Recital 22 of the AI Act states: 'To prevent the circumvention of this Regulation and *to ensure an effective protection of natural persons located in the Union*, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, *to the extent the output produced by those systems is intended to be used in the Union'*.

We argue that the same approach should apply to national security issues. These do not concern the territorial application of EU law, but we submit that a similar data-subject centric approach – already in place in the context of territorial matters – should be implemented to other questions of applicability of EU law as well. The next section discusses why this approach is needed by highlighting its underpinning normative foundation and its benefits. We then take a closer look at the potential limits and objections to that interpretation of EU data protection law, which concern national security and the lack of a legal basis. Consequently, it is necessary to consider possible ways of overcoming these limitations both under *de lege lata* and *de lege ferenda* perspectives. This discussion is undertaken drawing inspiration from digital constitutionalism, which constitutes the theoretical framework within which we develop our data-subject model.

4.3. Normative foundation and the benefits of the *data subject* model

The data subject model has a number of benefits. These are based on both descriptive and normative arguments.[128] Starting from the more descriptive benefits, the data-subject approach provides a clear and straightforward conceptualisation of the applicability of EU data protection law in the context of national security: This would apply where national security measures involve the monitoring of the behaviour or the processing of personal data of data subjects within the EU. In this regard, the data subject model would address the uncertainties – identified above – surrounding the current controller model which is based on blurred distinctions between private and public functions, as well as the uncertainties regarding the nature of the specific national security measure, as interpreted by the CJEU (broadly) or the EU legislator (narrowly). Legal clarity is urgently needed in this area where the case law of the Court – albeit welcome – has, regrettably, confused the current legal situation even further and has often resulted in a clear pushback from national governments and Supreme Courts, as in the case of France.[129]

[127] Emphasis added.
[128] These are not (and cannot be) totally separated.
[129] See above.

Secondly, the data subject model *aligns better* with the underlying aims of EU data protection law as it would bring into its scope of application new forms of intrusive surveillance that threaten fundamental rights and freedom at large yet remain excluded under the current controller model. It would, thus, serve better both the individual and social underpinning values and constitutional objectives of EU data protection law (and EU fundamental rights law more broadly).[130] This is significant because data protection has been elevated to the status of a fundamental right in the EU legal order (Article 8 Charter)[131] and is recognised in primary EU law (Article 16 TFEU) as an express legal basis for the adoption of data processing-related instruments, such as the GDPR.[132] The data subject model is, in this way, anchored in EU primary law rather than secondary EU law, where the Court's data controller approach is based.

Article 16 TFEU, in particular, has been relied upon to realise and promote respect for fundamental rights and freedoms in general (beyond data protection). For instance, it is noteworthy that the legal bases of the AI Act are: The internal market harmonisation clause (Article 114 TFEU) and Article 16 TFEU. As explained in Recital 3 of the AI Act, this secondary legal basis is justified insofar as the AI Act contains specific rules on data processing activities, particularly those 'concerning restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement'. The choice of Article 16 TFEU as a legal basis for the AI Act has not been uncontroversial; for example, Ebers et al, have questioned to what extent this provision can support the bans on certain AI systems whereby the aim is not only to protect the processing of personal data but more broadly fundamental rights and the democratic society.[133] However, as explicitly stated in the GDPR, the fundamental right to personal data protection seeks to protect people's fundamental rights and freedoms at large.[134] It is also commonly argued that the right to personal data protection aims at providing individuals with substantial control over their personal data and empowering them against informational power asymmetries.[135] It is

[130] See also below discussion on art 16 TFEU and on digital constitutionalism.

[131] M Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017); M Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a Not So New Right' (2013) 3 *International Data Privacy Law* 88.

[132] Art 16 TFEU.

[133] M Ebers, VRS Hoch, F Rosenkranz, H Ruschemeier and B Steinrötter, 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4 *J – Multidisciplinary Scientific Journal* 589, 590.

[134] Art 1(2) GDPR.

[135] See for example Tzanou (n 131); O Lynskey, 'Deconstructing Data Protection: The "Added Value" Of A Right To Data Protection In The EU Legal Order' (2014) 63 *The International and Comparative Law Quarterly* 569; J Ausloos, *The Right to Erasure in EU Data Protection Law* (Oxford University Press 2020); P Vogiatzoglou and P Valcke, 'Two Decades of Article 8 CFR: A Critical Exploration of the

therefore unsurprising that the European Parliament suggested bans on AI systems to protect individuals' rights not only with regard to personal data protection but also with regard to other fundamental rights, including privacy, non-discrimination, dignity and presumption of innocence.[136] The Parliament's position to the AI Act, relying on its legal basis being Articles 114 and 16 TFEU, to establish bans on technologies that present risks to human dignity and rights, demonstrates the instrumental role of personal data protection in safeguarding democratic values and rights, which the data-subject model promotes. While Article 16 TFEU is still bound by the EU's existing competence, as argued above, any exceptions to the exercise of the right to personal data protection in line with EU primary law cannot be unilaterally and in general terms decided by Member States, even for national security purposes.

The normative argument that follows from the above is that the grounding of the scope of applicability of EU data protection law should be removed from the data retention context and, indeed, from secondary EU law (the EPD) altogether. Article 15(1) of the EDP has long been relied on by the Court to bring relevant national security measures within the scope of applicability of EU law, but this is neither sufficient nor necessary. It is not sufficient because it would not capture new forms of surveillance, such as Palantir and Pegasus discussed in the case studies above. It is not necessary because within the digital constitutionalism framework discussed above, the applicability of EU data protection law on such important issues, such as national security, should be grounded on primary EU law and not on secondary law instruments, such as Directives, and the judicial or legislative interpretation thereof which is potentially subject to constant change. The grounding of the scope of application of EU data protection law on primary EU law through the data-subject model proposed is, therefore, needed as it would reduce the risk of EU data protection law becoming toothless and, hence, irrelevant in the face of new technological developments and new forms of surveillance.

Third, distinctions in the applicability of EU fundamental rights protections risk undermining the overall internal coherence of EU law[137] and should be avoided. In

Fundamental Right to Personal Data Protection in EU Law' in E Kosta, R Leenes and I Kamara (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 11.

[136] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Recitals 26(a) and 26(b).

[137] See *inter alia* J Raz, 'The relevance of coherence' (1994) 72 *Boston University Law Review* 273; R Dworkin, *Law's Empire* (Harvard University Press 1986) 166; J McGarry, 'The Possibility and Value of Coherence' (2013) 34 *Liverpool Law Review* 17; R Alexy and A Peczenik, 'The Concept of Coherence and Its Significance for Discursive Rationality' (1990) 3 *Ratio Juris* 130; A Schiavello, 'On "Coherence" and "Law": An Analysis of Different Models' (2001) 14 *Ratio Juris* 233; K Kress,

practical implementation terms, this issue has already arisen in the context of international data transfers which concern the question of the (extra-)territorial application of EU fundamental rights law to national security measures of third countries, such as the US. In this context, the EU has been accused – by mainly American commentators – of 'double standards'.[138] This is because the CJEU has confirmed the applicability of EU fundamental rights to US national security measures, when it is – to say the least – much less clear when EU fundamental rights apply to its own Member States' national security surveillance measures,[139] as the discussion above has demonstrated. There is, therefore, an overarching normative argument that underpins the proposed data subject centric approach: EU data protection law *should* be overall coherent and distinctions and exceptions between different elements of this law that introduce divergent rules for territorial and national security applicability *should* be removed. The *data-subject* model would end any such divergences in the review and scrutiny between Member States' and third countries' national security measures and the concomitant accusations of double standards and 'hypocrisy' from the EU's side in this regard.[140]

Finally, in practical terms, the adoption of the data-subject centric approach would create disincentives for Member States to 'baptise' a growing number of measures as pertaining to national security in order to escape the application of EU fundamental rights law.[141] Where such measures involve the monitoring of the behaviour or the processing of personal data of data subjects within the EU, they should come within the scope of application of EU fundamental rights law.

'Coherence and Formalism' (1993) 16 *Harvard Journal of Law and Public Policy* 639; K Kress, 'Coherence' in Dennis Patterson (ed), *A Companion to Philosophy of Law and Legal Theory* (Wiley-Blackwell 2010) 521; N MacCormick, 'Coherence in Legal Justification' in A Peczenik, L Lindahl and B van Roermund (eds), *Theory of Legal Science. Proceedings of the Conference on Legal Theory and Philosopy of Science Lund, Sweden, December 11-14, 1983* (Springer 1984) 235; R Grantham and D Jensen, 'Coherence in the Age of Statutes' (2016) 42 *Monash University Law Review* 360; B Baum Levenbook, 'The Role of Coherence in Legal Reasoning' (1984) 3 *Law and Philosophy* 355.

[138] S Baker, 'How Can the U.S. Respond to Schrems II?' (Lawfare, 21 July 2020), at www.lawfaremedia.org.

[139] On this point, see M Tzanou, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in F Fabbrini, E Celeste and J Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing 2020) 114; M Tzanou, 'Who Occupies the Transatlantic Data Privacy Space? Unpacking the Evolving Dynamics, and Assessing the Way Forward' in E Fahey (ed) *The Routledge Handbook on Transatlantic Relations* (Routledge 2023) 266.

[140] Ibid.

[141] We thank Niovi Vavoula for her insightful comment on this matter on an earlier draft of this article.

4.4. Addressing the objections to the *data subject* focused model

We acknowledge that while the proposed *data subject* model could resolve the legal uncertainties that arise in the context of national security and ensure that this does not become a law-free area, several objections could be raised against this model. We address the two main potential oppositions to our proposed approach.

A first and obvious objection concerns Article 4(2) TEU, which provides that 'national security remains the sole responsibility of each Member State'. Critics to the proposed data subject model would be quick to point out that this would be incompatible with the national security exception enshrined in EU primary law. While this is a valid and important objection, we submit, however, that it is not insurmountable. As mentioned above, through its data retention jurisprudence, the CJEU has clearly established that: 'although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, *the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law*.'[142]

The data subject model does not depart from this approach.[143] It is indeed based on exactly the same premise, with the mere difference that it focuses directly on protecting the data subject rather than on unclear definitions of private entities' involvement. This means that under the model proposed in this article, Member States would still be free to determine their security interests and adopt relevant national security measures they deem appropriate. Whenever such measures monitor the behaviour or more broadly process the personal data of EU data subjects, they would fall within the scope of application of EU law and the review of the Court as to their compatibility with EU fundamental rights- as is the current situation with data retention measures.

The most important objection that might be potentially raised against the proposed data subject approach is that this model is not based on the law. It thus differs from the controller model developed by the CJEU in its data retention case law which is based on Article 15(1) EPD which permits the adoption of national laws that restrict the confidentiality of electronic communications for national (and public) security purposes. The lack of a clear legal basis is a very important issue and we do not pretend to have an easy solution. However, we argue that there are possible ways

[142] *La Quadrature du Net and Others* (n 4) para 99.

[143] This approach is also confirmed in the law. As the CJEU has explained in *La Quadrature du Net and Others* (n 4), Directive on privacy and electronic communications (n 15) Art 1(3) excludes from its scope 'activities of the State' in the areas of public security, defence and State security (the 'exclusion' clause); while, Directive on privacy and electronic communications (n 15) Art 15(1) permits the adoption of national laws that restrict the confidentiality of electronic communications appropriate for national and public security purposes ('limitation' clause). See Tzanou and Karyda (n 29) 128.

of overcoming this limitation both *de lege lata* and *de lege ferenda*. We start from a *de lege ferenda* perspective and then move to a *de lege lata* discussion, which draws inspiration from the digital constitutionalism framework discussed above.

De lege ferenda, a shift to the data-subject model would require the intervention of the EU legislator. The data-subject model could be clearly enshrined in the law by a legislative amendment to the GDPR and the LED , the two core data protection instruments. We consider this probably the best solution as it would address the underlying problems identified above. First, it would bring legal certainty to an area dominated by conflicting judgments of the CJEU, fraught with unclear boundaries, conceptual confusion and inconsistencies. Second, it would ensure the overall coherence of EU data protection law by putting an end to divergences in its applicability depending on the context: this would apply both territorially and to national security matters, and it would be anchored in robust protections of fundamental rights enshrined in primary EU law. Third, from an internal market perspective, the varied deployment of modern surveillance methods[144] might lead to fragmentation in fundamental rights protection in the EU, which might have an impact on competition in the single market. Thus, from this perspective as well, a harmonised approach adopted by the EU legislature would be more desirable while ensuring an equal level of protection of fundamental rights.

Nevertheless, we acknowledge that a legislative intervention does not seem very realistic at the moment. Indeed, it appears that the intention of the EU legislator (in particular, the Council) is to delimit the impact of the CJEU's data retention judgments and to circumvent their consequences.[145] It should be recalled, however, that even the EU legislator has recognised that national security restrictions fall within the scope of application of EU law under Article 23(1) (a) GDPR and 15(1) EPD. In our view, a legislative amendment would bring clarity and consistency in the area, while acknowledging that even if EU law is applicable to national security, there is still room for restrictions in this area and a significant margin of appreciation of Member States, as foreseen in the GDPR and also recognised by the CJEU.[146] Indeed, restrictions on data subject rights, for instance, are permitted for purposes of national security in line with Article 23 GDPR. As the data retention line of cases has further shown, mass surveillance is, in fact, allowed for national security but

[144] The PEGA Committee notes that these have been adopted by the Polish (Pegasus spyware), Hungarian (Pegasus spyware), Greek (Predator spyware), and Spanish (Pegasus spyware) governments, adding that 'it can be safely assumed that all Member States have purchased or used one or more spyware systems'. PEGA, Recital O

[145] See Section 3.1.

[146] As the CJEU acknowledges, national security is considered the most important objective of general interest and is capable of justifying measures entailing what are considered the more serious interferences with fundamental rights. *La Quadrature du Net and Others* (n 4) para 136.

subject to certain safeguards.[147] It would certainly be more honest for the EU legislator to directly recognise the applicability of EU law to national security measures and ensure that certain safeguards are needed – even in this area – to maintain democratic societies. This also aligns with the national obligations deriving from the ECHR, as discussed above.[148]

From a *de lege lata* perspective, we argue that a data subject centric interpretation of EU law would be possible. Going back to the digital constitutionalism framework discussed above, we argue that the adoption of the data subject model would further the constitutionalisation process which has begun by the Court.[149] We consider that there are common foundational values, motivations and aims between our model and the Court's approach when seen through the prism of digital constitutionalism: fundamental rights protection- even if not mentioned explicitly by the Court in its data retention case law as far as the scope of application of EU law is concerned. As mentioned above, constitutionalisation is a dynamic process comprising different stages. The data retention case law has institutionalised the application of EU law to national security. However, we view this as the beginning, rather than the end of the constitutionalisation process in the area.[150] Challenges posed by new forms of surveillance require a rethinking of the developed normative counteractions. Our data-subject model offers a new normative answer that is now explicitly based on primary EU law, more specifically on Article 8 Charter and Article 16 TFEU. A model that is centred on the data subject is an approach required by fundamental rights and constitutional norms. Therefore, in our view, such an interpretation would be possible also from a *de lege lata* perspective. Grounding the application of EU law to national security surveillance technologies – old or new – directly on the fundamental right to data protection (rather than obscure secondary law provisions) is the next step in this dynamic constitutionalisation process. After all, we can already observe 'a new evolving trend in EU policy, characterized by the extension of constitutional values

[147] Ibid.

[148] As the ECtHR in particular notes, '[a] measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal.' *Szabó and Vissy v Hungary* App n. 37138/14 (ECtHR, 6 June 2016) para 73.

[149] See also O Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Hart Publishing 2021).

[150] See also M Tzanou, 'The Judicialization of EU Data Retention Law: Epistemic Injustice and the Construction of an Unequal Surveillance Regime' in E. Kosta and I. Kamara (eds) *Data Retention in Europe and beyond: Law and Policy in the aftermath of an invalidated directive* (Oxford University Press 2025) 343.

beyond EU borders'. [151] An articulation of a similar human-centric technological model concerning its Member States as well is, hence, both urgently needed and well anchored in primary EU law foundations.

5. Conclusions

National security is a complex regulatory area that brings together public and private actors performing a variety of functions for the safeguarding of the Member States' national interests. Although this area remains the sole responsibility of Member States, the CJEU's rulings on data retention have extended the applicability of EU data protection law to national security activities when those involve private entities – ECSPs – subject to EU law. Albeit welcome from a fundamental rights' perspective, this interpretation of the scope of EU law raises a number of questions. More specifically, the Court relied on a fluctuating understanding of what constitutes an ECSPs' activity, from data retention, to provision of access to data, to all processing operations undertaken by the providers themselves, be it for public or national security. As all ECSP activities, even for national security purposes, must also abide by EU law standards, national security is no longer an EU (fundamental rights) law free area. However, the applicability of data protection safeguards onto national security activities is far from settled. First, the EU legislator is trying to circumvent the EU Court's jurisprudence altogether. On the basis of the EU Treaties which appoint sole responsibility on matters of national security to Member States, the EU legislator has introduced a new exemption clause to the regulation of artificial intelligence. The clause clarifies that national security activities are exempted from EU law regardless of the (private) actor carrying it out.

Second, the operational reality of electronic communications surveillance paints a much more blurred picture, whereby it is increasingly difficult to discern between purely governmental state activities for national security and private actor activities. New forms of surveillance technologies, such as Palantir and Pegasus have revealed a crucial weakness of the above regulatory approach: while they implicate the involvement of private companies, EU fundamental rights are not applicable at all to such surveillance systems as they do not involve the retention of data by ECSPs. It shows, therefore, that the current regulatory framework in the area of national security as interpreted by the Court is no longer fit for purpose. It relies on shaky grounds as it is bound to be circumvented by the EU legislator and overall falls short from achieving the overarching fundamental goals of EU fundamental rights law that are to protect both individual data subjects from such invasive (new forms of) surveillance and to ensure the overall functioning of the rule of law and a democratic society.

[151] De Gregorio (n 108) 67.

An urgent need, thus, arises to rethink the current regulatory framework so that this can deal with new forms of surveillance and address the uncertainties that the CJEU's data retention case law has created. Digital constitutionalism offers an appealing theoretical framework for this endeavour. Constitutional theory, including both its traditional[152] and more innovative articulations,[153] offers a 'prism'[154] through which scholars can study ongoing phenomena[155], and reflect on future directions.[156] Digital constitutionalism requires us to develop new ways of limiting abuses of power in a complex system that includes many different governments and private actors. We propose a new approach, the *data subject centric model*, as a normative counteraction of constitutional nature – a reaction based on constitutional law against the power emerging from digital technologies. Our approach differs from current EU approaches to the national security problem, which are based on secondary law and in particular the interpretation of the EPD. Its ultimate aim is to achieve 'constitutional equilibrium', thus it is strongly anchored on fundamental rights (Articles 7 and 8 Charter) and other provisions of primary EU law (Article 16 TFEU).[157] Our proposal focuses on two basic aspects of digital constitutionalism (and constitutional law in general): the protection of fundamental rights and the balancing of powers. It sees the applicability of EU fundamental rights to national security measures as a pre-condition for the achievement of the constitutional equilibrium in this area, without which the substantive fundamental rights protection cannot be realised. The data subject model envisages the applicability of EU law to national security measures where these involve the monitoring of the behaviour or the processing of personal data of data subjects within the EU. While this model is innovative, it is not unfeasible from a legal point of view. As explained, it draws inspiration from current approaches of the law, including the rules on the territorial application of the GDPR (Article 3(2) GDPR).

The data subject model has several benefits. First, it provides a clear and straightforward conceptualisation of the applicability of EU data protection law in the context of national security, thus, addressing the uncertainties of the current controller model while advancing better the constitutional foundations of EU data protection law. Second, it is founded, in accordance with digital constitutionalism, on EU primary law. This means that it removes the grounding of the scope of applicability of

[152] M Loughlin, 'What Is Constitutionalisation?' in P Dobner and M Loughlin (eds) *The Twilight of Constitutionalism?* (Oxford University Press 2010) 47.

[153] A Wiener, AF Lang Jr, J Tully, MP Maduro and M Kumm, 'Global Constitutionalism: Human Rights, Democracy and the Rule of Law' (2012) 1 *Global Constitutionalism* 1.

[154] Celeste (n 107).

[155] Ibid.

[156] Peters (n 121).

[157] Celeste (n 107).

EU data protection law from the data retention context and, indeed, from secondary EU law – the EPD – altogether. It is therefore, able to capture new forms of surveillance, such as Palantir and Pegasus, and to reduce the risk of EU data protection law becoming toothless and, hence, irrelevant in the face of new technological developments. Third, the model would make EU data protection law more coherent, avoiding divergences in the application of fundamental rights depending on context (territorial applicability and national security applicability).

There are different ways through which the data subject model could be taken forward. The best approach would be for the EU legislator to directly recognise the applicability of EU law to national security measures and ensure that certain safeguards are needed – even in this area – to maintain democratic societies. Nevertheless, we acknowledge that such a legislative intervention does not seem very realistic at the moment. The article, therefore, submits from a *de lege lata* perspective, that the adoption of the data subject model would further advance the constitutionalisation process which has already begun by the Court through its data retention jurisprudence.

Overall, we recognise that the shift to the proposed *data subject-focused* approach requires bold and courageous steps from the CJEU or the EU legislator. However, it is urgently needed in face of new forms of surveillance, such as Pegasus, which require, in the words of the EDPS, 'to rethink the entire existing system of safeguards established to protect our fundamental rights and freedoms, which are endangered by these tools'.[158] This article argued that this rethinking must be undertaken by putting *data subjects* and *their fundamental rights* at the forefront; even in the context of national security.

[158] European Data Protection Supervisor (n 1) 2.