Effective Data Protection and Direct Cooperation on Digital Evidence

Gavin Robinson

Assistant Professor, Willem Pompe Institute for Criminal Law and Criminology and Utrecht Centre for Shared Regulation and Enforcement in Europe (RENFORCE), Utrecht University, The Netherlands.

**Chapter forthcoming in* Vanessa Franssen & Stanisław Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (CUP).

Keywords: data protection, direct cooperation, digital evidence, GDPR, LED, European Production Order, ePrivacy

Abstract:

This chapter explores the relationship between EU data protection law and public-private 'direct cooperation' on digital evidence in criminal investigations. It asks whether a prima facie neat separation between the GDPR and the LED always matches the realities of private-to-public data transfers for criminal investigations, and questions whether that legal framework is sufficiently harmonious to warrant description as an EU data protection *acquis*. The chapter distinguishes scenarios of formal (and informal) direct cooperation, viewing those scenarios through the conceptual prism of data controllership. That frame is then applied to the European Commission's 2018 'e-Evidence package', along with the other co-legislators' competing visions, before a first look at the final 2023 compromise text from a data protection perspective. The chapter analyses the extent to which CJEU case law illuminates theoretical blind spots, and critically discusses whether the ongoing strengthening of enforcement powers is likely to herald not only greater legal certainty on the supply of digital evidence but also meaningful, workable data subject rights. The chapter closes with a reflection on the future place of EU data protection standards within the Council of Europe's own new direct cooperation mechanism – that of the Second Additional Protocol to the Budapest Convention.

1. Introduction

Criminal investigations and proceedings substantiate and establish the innocence or guilt of a (traditionally, natural) person in respect of suspicions of criminal conduct or specified criminal charges. Accordingly, putative digital evidence sought by police and judicial authorities – whether in the domestic or cross-border setting – will very often qualify as personal data, defined in the EU General Data Protection Regulation (GDPR)[1] as any information:

> '(…) relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'[2]

Furthermore, chains of cooperation between private actors (for instance, 'tech' companies) and public authorities (classically the police, prosecutors, judges or courts) involve multiple instances of data processing, defined in the GDPR as:

> '(…) any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[3]

In recent years, the imperative to access digital evidence (and thus personal data) has driven intense policy- and law-making activity on both sides of the Atlantic. A particular focus therein has been on streamlining the cross-border obtention of communications data from (tele)communications service providers.

2018 stands out, as the year which saw the passing of the CLOUD Act[4] in the USA and the release of the European Commission's 'e-Evidence package'.[5] At the time of writing the bulk of this chapter, the latter proposal remained locked in trilogue negotiations more than four years on – although the summer of 2022 heralded a breakthrough, before a final compromise text emerged in early 2023.[6] Over at the Council of Europe, lengthy negotiations on a Second Additional Protocol (2nd Protocol) to the 2001 Cybercrime Convention (Budapest Convention)[7] came to fruition in November 2021.[8] Whilst those three developments differ in many important respects, they all share a gradualist (and contested) enshrinement of an enforceable legal

[1] 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), [2016] OJ L 119, 4 May 2016, p. 1–88.

[2] GDPR, Art. 4(1).

[3] GDPR, Art. 4(2).

[4] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V (2018) (enacted) amending various parts of Title 18 (United States Code) U.S.C., including Chapter 121.

[5] European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (Draft e-evidence Regulation), [2018] COM(2018) 225 final, 17 April 2018; European Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (Legal Representatives Directive, draft LRD), [2018] COM(2018) 226 final, 17 April 2018.

[6] As will be unpacked at Section 4.1 below.

[7] Council of Europe, *Convention on Cybercrime* (Budapest Convention), ETS No. 185, 23 November 2001.

[8] In May 2022, the 2nd Protocol was opened for signature by the Parties to the Convention; *see,* European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, [2022] OJ L 134, 11 May 2022, available at: https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention.

mechanism for so-called 'direct cooperation' across territorial borders, meaning the 'unmediated'[9] serving by criminal investigators (with or without prior judicial authorisation) of binding orders for the production of data in one jurisdiction on private entities based or represented in another jurisdiction – without involving or potentially even informing the relevant local authority.

Another of the mentioned reforms' points in common tends, on the other hand, to be conspicuous by its absence from the policy debates: whilst the ongoing policy drive aims at achieving faster, more efficient and more reliable cross-border access to data, there is a dearth of specific treatment of the intertwined data protection issues.

Indeed, to the extent that data protection has entered the 'e-evidence debate', the greater mass of policy and scholarly attention has so far focused on the paradigmatic transatlantic cases of '*Microsoft Ireland'* (US investigator, data in Europe)[10] and *'Yahoo! Belgium'* (EU Member State investigator, provider and data in the USA).[11] The ramifications of the *Schrems*[12] jurisprudence from the Court of Justice of the European Union and the future of data transfers from the EU to the USA post-CLOUD Act also loom large in expert commentary.[13] This is understandable, not least given the dominance of US-based tech companies on the EU market and the legitimate sense of urgency caused by the absence of a framework for data sharing from the EU to the USA since the – equally legitimate, and moreover inevitable – annulment of the Privacy Shield by the Court of Justice of the European Union (CJEU) in *Schrems II.*[14]

Yet a policy drive locked on removing legal obstacles to enforceable cross-border production orders and expert debates on the flux surrounding transatlantic data transfers risk overlooking the broader impacts of the as-yet-inchoate paradigm shift toward formalised direct cooperation on data protection standards in other 'direct cooperation' scenarios: namely, those involving other third states, intra-EU cases, and direct cooperation in purely 'domestic' cases.

---

[9] Distinguishing 'mediated', 'unmediated' and 'hybrid' models of access to electronic data. *See,* S. Carrera, G. González Fuster, E. Guild, and V. Mitsilegas, 'Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights', *Centre for European Policy Studies*, 8 July 2015, available at: https://www.ceps.eu/ceps-publications/access-electronic-data-third-country-law-enforcement-authorities-challenges-eu-rule-law/.

[10] *Microsoft Corp.* v. *United States,* 829 F.3d 197 (2d Cir. 2016); *see,* X., 'Privacy – Stored Communications Act – Second Circuit Holds that the Government Cannot Compel an Internet Service Provider to Produce Information Stored Overseas' (2016) 130 *Harvard Law Review,* 2, 769-776. On appeal, the case was vacated by the U.S. Supreme Court as *United States* v. *Microsoft Corp.,* 584 U. S. (2018) following passage of the CLOUD Act in March 2018.

[11] Cour de cassation (Belgian Supreme Court), 1 December 2015, P.13.2082.N. . Covering both '*Yahoo! Belgium'* and '*Microsoft Ireland', see,* P. De Hert, C. Parlar and J. Thumfart, 'Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland' (2018) 9 *New Journal of European Criminal Law,* 3, 326-352. *See also,* F. Verbruggen and S. Careel in this volume.

[12] Case C-498/16 *Maximilian Schrems v Facebook Ireland Limited* [2018] ECLI:EU:C:2018:37 ('*Schrems I*'); Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems* [2020] ECLI:EU:C:2020:559 ('*Schrems II*'). *See,* V. E. L. Cervantes, 'The Schrems II Judgment of the Court of Justice Invalidates the EU – U.S. Privacy Shield and Requires 'Case by Case' Assessment on the Application of Standard Contractual Clauses ('SCCs')' (2020) 6 *European Data Protection Law Review*, 4, 602-606.

[13] *See,* P. Swire, 'When does GDPR act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer', *Cross-Border Data Forum,* 4 November 2019, available at: https://www.crossborderdataforum.org/when-does-gdpr-act-as-a-blocking-statute-the-relevance-of-a-lawful-basis-for-transfer. *See also,* T. Christakis, 'Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?', in R. Milch and S. Benthall (eds.), *Cybersecurity and Privacy in a Globalized World – Building Common Approaches* (New York University School of Law, e-book), *forthcoming*, chapter available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3397047.

[14] In March 2022 the European Commission and the United States announced an agreement in principle on a new 'Trans-Atlantic Data Privacy Framework', and in October 2022 US President Biden issued an 'Executive Order on Enhancing Safeguards for United States Intelligence Activities' to pave the way for the establishment of a new 'Data Protection Review Court'. At the time of writing, the Commission envisaged moving to the next steps, including proposing a draft adequacy decision and launching its adoption procedure, *See,* European Commission, 'Questions & Answers: EU-U.S. Data Privacy Framework', 7 October 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

Indeed, even where a criminal case involving digital evidence is in all core respects – investigating authority, suspect, victims, data and third parties in control of that data – local, meaning there is no need to reach beyond the national territorial borders of one EU Member State in the course of investigations, EU data protection law already comes into play. The starting point is that the stronger GDPR standards apply to the private parties called upon to cooperate with criminal investigators, and the weaker standards in the so-called 'Law Enforcement Directive' (LED)[15] – as implemented in national law – apply to the latter.

But what does the coexistence of the GDPR and the LED imply for direct cooperation on digital evidence? Does a prima facie neat separation between the two instruments always match the realities of private-to-public data transfers? Is the legal framework sufficiently harmonious to fully warrant description as an EU data protection *acquis*? How far can the evolving case-law of the CJEU take us in illuminating blind spots, and what are the prospects for the ongoing strengthening of enforcement powers heralding greater legal certainty regarding not only the supply of digital evidence but also the applicable data protection laws, extending to meaningful, workable data subject rights?

Those are the tensions, underexamined in both policy and academic debates, which this chapter aims to explore.

The chapter's focus is on direct ('unmediated') *cooperation* with *third parties* in control of data pertaining to the target of investigations or proceedings – although indirect or 'mediated' cooperation will also be mentioned where instructive. As such, it touches only in passing on the obtention of digital evidence 'directly' from the target, whether in the context of consensual 'transborder access' to data,[16] the search and seizure of digital devices and of data,[17] or so-called police hacking. At the same time, the chapter stakes no claim as to the (empirical)[18] case made for the necessity of new direct cooperation powers at EU level as opposed to a less radical 'express EIO[19] for data',[20] or tackle the long list of possible improvements to the mutual legal assistance (MLA) systems already in place for most cooperation beyond the Union.[21]

Especially since the endowment of the Charter of Fundamental Rights of the European Union[22] with the same legal value as the Treaties,[23] it can often seem that almost every conceivable facet of a putative direct cooperation mechanism can be connected to the 'all-

[15] 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 (LED), [2016] OJ L 119, 4 May 2016, p. 89–131.

[16] *E.g.,* Budapest Convention, Art. 32b, pursuant. *See further,* N. Seitz, 'Transborder Search: A New Perspective in Law Enforcement?' (2005) 7 *Yale Journal of Law & Technology,* 1, 23-50.

[17] *See,* G. Lasagni in this volume. M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence: Toward Common European Standards in Antifraud Administrative and Criminal Investigations* (Milan: Wolters Kluwer / CEDAM, 2021).

[18] For a critical view, *see,* G. González Fuster and S. Vázquez Maymir, 'Cross-border access to E-Evidence: Framing the Evidence', *Centre for European Policy Studies*, 2 March 2020, available at https://www.ceps.eu/ceps-publications/cross-border-access-to-e-evidence/.

[19] 'EIO' refers to Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive), [2014] OJ L 130, 1 May 2014, p. 1 – 36.

[20] *See,* in detail in this volume, T. Christakis; and, comparing co-legislators' positions on key elements of the reform, K. Ligeti and G. Robinson, 'Sword, Shield and Cloud: Toward a European System of Public-Private Orders for Electronic Evidence in Criminal Matters?', in V. Mitsilegas and N. Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Oxford: Hart Publishing, 2021).

[21] *See e.g.,* S. Tosza, 'Cross-border gathering of electronic evidence: Mutual legal assistance, its shortcomings and remedies', in V. Franssen and D. Flore, *Société numérique et droit pénal* (Brussels: Larcier/Bruylant, 2019), pp. 269-285.

[22] Charter of Fundamental Rights of the European Union (Charter), [2012] OJ C 326, 26 October 2012, pp. 391-407 (Charter).

[23] Treaty on European Union (TEU), [2016] OJ C 202, 7 June 2016, Art. 6(1).

overriding fundamental (super-)right'[24] to personal data protection under its Article 8. The chapter does not aim to inventory all such issues. Data security and related organisational and technological measures required in order to seamlessly send data between (duly-authenticated[25]) actors in the course of criminal investigations will not be addressed.[26] Likewise, ongoing infrastructural, practical or training efforts to (further) digitalise cross-border justice[27] and police cooperation[28] within the EU will not be seen in any detail.

The aim is rather to further the discussion on the potential impact of direct cooperation on digital evidence in criminal matters on two of the three cornerstones of EU data protection law, as enshrined in Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 8 of the Charter: data processing principles and data subject rights.[29]

As both of these interrelated foundations of EU data protection law flow from the applicable rules, that is where the analysis begins in Section 2, with a presentation of the main plinths of the current EU legal framework. Thereafter, the interactions between that legal framework and direct public-private cooperation on digital evidence are explored in Section 3, before the significance from a data protection perspective of ongoing reforms at EU and Council of Europe level is discerned in Section 4. Section 5 offers some concluding remarks.

2. Main plinths of the EU data protection *acquis*

Although in 2009 the Lisbon Treaty, in collapsing the pillars of the Union, brought a new horizontal legal basis for data protection in Article 16 TFEU and elevated the right to data protection in the Charter to constitutional level[30] the political rider in Declaration no. 21 to the Lisbon Treaty concerning the fields of judicial cooperation in criminal matters and police cooperation already hinted that the next generation of EU legislation on data protection was

[24] Opinion of Advocate General Bobek in Case C-175/20, *SIA 'SS' v Valsts ieņēmumu dienests*, 2 September 2021, ECLI:EU:C:2021:690, para 2. *See also*, in detail, N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10 *Law, Innovation and Technology,* 1, 40-81.

[25] Lest, for instance, impersonators should successfully serve 'official' orders on unsuspecting service providers. *See e.g.,* W. Turton, 'Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests', *Bloomberg*, 30 March 2022, available at: https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests.

[26] See for instance European Data Protection Supervisor, 'Opinion 7/2019 EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matter' (EDPS e-Evidence Opinion), 6 November 2019, paras. 33-38 insisting on the need for verification of the authenticity of certificates and orders, security of transmission of certificates and the requested data, and that provisions on identifying authorities emitting orders and legal representatives receiving them should be active before system launch in order to reduce risks of personal data breaches.

[27] In 2022, most Member States are expected to begin using 'e-EDES' (the e-Evidence Digital Exchange System, European Commission) for electronic transmission of European Investigation Orders (EIOs), which may be used in order to obtain digital evidence; Eurojust is also preparing to connect to and possibly use e-EDES. *See,* Eurojust, 'Annual Report 2021', 2 March 2022, p. 67, available at: https://www.eurojust.europa.eu/publication/annual-report-2021-20-years-criminal-justice-across-borders.

[28] In December 2021, the Commission proposed an EU Police Cooperation Code including a draft Directive on information exchange between law enforcement authorities of Member States, repealing the so-called 'Swedish Framework Decision' from 2006 and a draft Regulation on automated data exchange for police cooperation (Prüm II); see Press Release, 'Boosting police cooperation across borders for enhanced security', European Commission, 8 December 2021, available at: https://home-affairs.ec.europa.eu/news/boosting-police-cooperation-across-borders-enhanced-security-2021-12-08_en.

[29] The third cornerstone, independent supervision, is largely left to future research efforts. *See,* P. De Hert and J. Sajfert in 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data', in C. Brière and A. Weyembergh, *The Needed Balances in EU Criminal Law. Past, Present and Future* (Oxford: Hart Publishing, 2018), p. 250.

[30] TEU, Art. 6(1).

to retain some level of 'pillarisation'[31] well into the future, due to the 'specific nature' of those two fields.[32]

So it materialised, with the GDPR thus now in place for service providers' handling of customers' personal data,[33] and the LED applying 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, including the safeguarding against and the prevention of threats to public security'.[34]

Therefore, whenever data is transferred by private actors to the competent authorities, *a priori* this entails a switch of data protection regime: the data 'travel' from the GDPR regime to the LED regime as implemented in national law. Whether and to what extent this is always the case in different scenarios of public-private cooperation will be examined in greater detail in Section 3, below. First, however, it is necessary to prepare the ground with a brief comparison of the scope and levels of protection offered by each legal instrument.

2.1. The GDPR and ePrivacy reform

Pursuant to Article 2(2) of the GDPR, the Regulation does not apply to four types of personal data processing, two of which are most relevant for present purposes: processing in the course of an activity which falls outside the scope of Union law (Article 2(2)(a)) and processing 'by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (Article 2(2)(d)). This exception thus mirrors word-for-word the material scope of its sister instrument, the LED, as set out above. The GDPR does apply, however, when competent authorities process personal data for purposes other than what might be called 'LED purposes', '*including* for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law'.[35]

Although the GDPR does not apply to law enforcement actors when discharging their core duties, law enforcement capacities are directly impacted by its growing influence on the private actors who are the source of much digital evidence. In particular it seems inevitable that full realisation of the data minimisation principle would mean less data available for criminal investigations.[36] A prime example, of key value in practice and carefully detailed by the European Commission in a dedicated Annex to its Impact Assessment accompanying the e-Evidence package, is the WHOIS directory service for domain names, part of which has (controversially) long remained publicly-accessible.[37] With the GDPR being applied from May 2018 onward and the uncertainty surrounding the suitable legal basis under the Regulation for such public access, ICANN has been grappling with how to ensure compliance without

[31] D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz and A. Scherrer, 'Fighting cyber crime and protecting privacy in the cloud', *European Parliament,* October 2012, p. 36, available at: https://pure.uva.nl/ws/files/1732778/148157_398380.pdf.

[32] Declaration no. 21, [2016] OJ C 202, 7 June 2016, p. 345.

[33] GDPR, Art. 2(1).

[34] LED, Arts. 2(1) and 1(1).

[35] LED, Art. 9(2), in conjunction with Recital 12. Emphasis added. We return to the precise contours of who or what might qualify as a 'competent authority' below.

[36] For a warning against the broader, potentially negative impacts of a strict application of the data minimisation principle on the practices of Big Data analysis across the board, *See,* T. Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 *Seton Hall Law Review* 1009-1012.

[37] European Commission, 'Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' (Draft e-Evidence Regulation and draft Legal Representatives Directive), SWD(2018) 118 final, 17 April 2018 (COM e-Evidence IA), Annex 12.

domain name registries having to move to closed systems,[38] causing an important investigatory starting point to dry up as a direct consequence of data protection enforcement.

The data minimisation principle also dovetails with the continued lack of an EU-level obligation on communications service providers to retain metadata for later use by law enforcement. The result is that investigations are hampered from the outset: typically, where an IP address has been obtained from a service provider, it will be necessary to ask an internet access provider (or, if it keeps logs, a VPN service provider) to determine who used defined IP addresses at specific times. Given the absence of an EU-level data retention regime in combination with a tightening of the data minimisation principle, the data may well be gone.[39]

Of course, the reason for the continued lack of a unified data retention obligation at EU level is well-known: the CJEU's seminal case law from *Digital Rights Ireland* (2014)[40] and *Tele2* (2016),[41] via *Privacy International*[42] and *La Quadrature du Net* (both 2020),[43] up to the recent judgments in *GD,*[44] *VD and SR*[45] and *SpaceNet* (all 2022),[46] with little sign of the multifaceted line of jurisprudence stopping there.[47] The pertinence of the Court's position(s) on communications data retention to the relationship between data protection and direct cooperation is analysed below in Section 3.2.

It suffices here to dwell briefly on the significance for direct cooperation of the ePrivacy Directive,[48] the legal instrument which 'particularises and complements' the standards set out in GDPR with respect to the processing of personal data in the electronic communication sector, and is at the heart of the CJEU's data retention case law since *Tele2.* Although the precise relationship between the exclusory clause in Article 1(3) and the limitation clause in Article 15(1) provide its pressure point, the root of the data retention dispute is found in Articles 6 and 9 of the ePrivacy Directive. Article 6 establishes the rule that traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of the communication, for billing and payments, or for marketing (with subscriber or user consent). Article 9, meanwhile, provides that 'location data other than traffic data' may only be processed when it is made anonymous or this is done with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.[49]

From 21 December 2020, the definition of the 'electronic communications services' (ECS) to which the above provisions apply was broadened by the introduction of the European

[38] European Data Protection Board, 'The European Data Protection Board endorsed the statement of the WP29 on ICANN/WHOIS', 27 May 2018, available at: https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en.

[39] COM e-Evidence IA, p. 23.

[40] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger* [2014] ECLI:EU:C:2014:238.

[41] 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* [2016] ECLI:EU:C:2016:970 (*Tele2*).

[42] Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790 (*Privacy International*).

[43] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others* [2020] ECLI:EU:C:2020:791 (*La Quadrature du Net*).

[44] Case C-140/20, *GD v Commissioner of An Garda Síochána and others* [2022] ECLI:EU:C:2022:258 (*GD*).

[45] Joined Cases C-339/20 and C-397/20, *VD and SR* [2022] ECLI:EU:C:2022:703 (*VD and SR*).

[46] Joined Cases C-793/19 and C-794/19, *Spacenet and Telekom Deutschland* [2022] ECLI:EU:C:2022:702 (*SpaceNet*).

[47] *See further,* S. Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of *La Quadrature du Net and others* and *Privacy International'* (2022) 8 *European Data Protection Law Review,* 1, 143-155.

[48] 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*)* (ePrivacy Directive)*,* [2002] OJ L 201, 31 July 2002, p. 37–47.

[49] ePrivacy Directive, Art. 5 is also a very important protection as it binds Member States to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications *and the related traffic data* by persons other than users, without the consent of the users concerned, except when legally authorised to do through legislative measures. Emphasis added.

Electronic Communications Code ('EEC Code')[50] to include so-called 'number-independent interpersonal communications services' (NI-ICS), which include OTT (over-the-top) services such as Voice-over-IP, messaging and web-based email services. According to McIntyre, the extension of the stronger confidentiality rules of Article 5 of the ePrivacy Directive to those services is likely to drive down voluntary disclosure to law enforcement and transfer greater pressure onto new schemes for formalised direct cooperation, particularly the EU e-Evidence package and the related EU-US agreement.[51]

OTT services will moreover be amongst the electronic communications services falling within the scope of the upcoming ePrivacy Regulation[52] which will eventually[53] replace the ePrivacy Directive. At the time of writing, the contents of the intensively-lobbied new Regulation, and in particular whether it will overall maintain, raise or lower the levels of protection afforded by the old Directive (an instrument dating back to 2002), remain uncertain. For present purposes, it is worth highlighting the following provision in the Council's 2021 mandate regarding the Regulation's material scope: Article 2.2(a) provides that it will not apply to:

> 'activities, which fall outside the scope of Union law, and in any event 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.'[54]

The wording of this provision as well as the timing of the mandate, four months on from the CJEU's decisions in *La Quadrature du Net* and *Privacy International,* leave little room for doubt that it was intended as a response to those rulings. In particular, the above provision squarely contradicts the Court's conclusion that the processing of personal data (including retention and transmission) by electronic communications service providers for the purpose of safeguarding national security falls within the scope of EU law – notwithstanding Article 4(2) TEU.[55] For the European Data Protection Board ('EDPB'), this aspect of the Council mandate 'runs against the premise for a consistent EU data protection framework';[56] whilst Tzanou and Karyda observe that 'circumventing – or indeed abolishing – the CJEU's jurisprudence on data retention in the ePrivacy Regulation would also set a dangerous precedent for the Court's assessment of third country metadata retention laws and practices, such as the US, in light of

[50] Directive (EU) 2018/1972 of the European Parliament and the Council of 11 December 2018 establishing the European Electronic Communications Code (EEC Code), [2018] OJ L 321, 17 December 2018 p. 36-214.

[51] T. J. McIntyre, 'Voluntary Disclosure of Data to Law Enforcement: The Curious Case of US Internet Firms, their Irish Subsidiaries and European Legal Standards', in F. Fabbrini, E. Celeste and J. Quinn (eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Oxford: Hart Publishing, 2021), p. 20. Implementation of the EEC Code appears to be slow. *See,* European Commission, 'EU Electronic Communications Code: Commission refers 10 Member States to the Court of Justice of the EU', 6 April 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1975.

[52] European Commission, Proposal for a Regulation 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), [2017] COM(2017) 10 final, 10 January 2017.

[53] At the time of writing, the latest available full text of the draft Regulation is the Council mandate from 10 February 2021. *See,* Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (ePrivacy Regulation Council mandate), [2021] 2017/0003(COD), 10 February 2021, available at: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[54] ePrivacy Regulation Council mandate, s. 42.

[55] *Privacy International*, para. 44. TEU, Art. 4(2) reads: 'The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. *In particular, national security remains the sole responsibility of each Member State*.' Emphasis added.

[56] Adding that '[i]n the event of an exclusion, the EDPB stresses nevertheless that the GDPR applies'.

Schrems I and *Schrems II*. Double standards in this regard risk rendering the CJEU's case law meaningless and cannot be accepted'.[57]

2.2. The Law Enforcement Directive

Although Recital 10 of the LED makes reference to the aforementioned Declaration no. 21 to the Lisbon Treaty – which referred only to police and judicial cooperation – the scope of the Directive goes beyond such cooperation in order to include domestic law enforcement processing, i.e. irrespective of whether data processing crosses national borders within the EU. For this reason alone, the LED constitutes a major upgrade on its predecessor, the 2008 Framework Decision, which only applied to cross-border processing.[58] In several other respects, however, as is well-established in the literature,[59] compared to the GDPR, the LED 'waters down'[60] the three cornerstones of EU data protection law: data processing principles, data subject rights, and independent supervision.[61]

The vicissitudes of political compromise required in order to reach an outcome on the LED, combined with the heterogeneity of authorities, tasks and powers in the 'law enforcement' area across the Member States, quickly prompted the academic literature to identify a host of reservations as to the approximation power of the instrument – beginning with its personal and material scope.

As concerns personal scope, the question is in the first place which public authorities qualify as 'competent authorities' under the LED.[62] Initial assessment of national implementations has suggested a wide divergence of approaches in the Member States: for instance, closed lists of public authorities contrast with open-ended provisions which could include local authorities, assessed on a case-by-case basis, whilst some national provisions may well encompass foreign public authorities.[63] The application of the LED to cross-border cooperation between national Financial Intelligence Units (FIUs) – which are classed as administrative authorities in some Member States, and law enforcement authorities in others – also warrants careful assessment.[64]

Regarding material scope, the wording of Recital 12 has enabled several national legislators to attach their LED-implementing rules (in place of the GDPR) to data processing relating to

---

[57] 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,* 1, 152-153.

[58] Compare Art. 1(1) and Recital 7 of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2008] OJ L 350, 30 December 2008, p. 60-71.

[59] T. Quintel and J. Sajfert, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities', in M. Cole and F. Boehm (eds.), *GDPR Commentary* (Cheltenham: Edward Elgar Publishing, *forthcoming*), chapter available at: https://ssrn.com/abstract=3285873. Castets-Renard presents the three main areas of weaknesses in the LED as (i) excessively supple directing principles, (ii) limited data subject rights, and (iii) inadequacy of data controller obligations (translation author's own). *See,* C. Castets-Renard, 'Directive 2016/680/UE et réforme des données personnelles en matière pénale : le droit européen en quête de protection et cohérence', in É. Debaets, A. Duranthon and M. Sztulman (eds.) *Les fichiers de police,* 1st Edition (Bayonne: Institut Universitaire Varenne, 2019), p. 401-419, 404-416.

[60] P. De Hert and V. Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A first analysis' (2016) 7 *New Journal of European Criminal Law,* 1, 18.

[61] *See further*, De Hert and Sajfert, 'The Role of the Data Protection Supervisory Authorities', pp. 244-247.

[62] The question of whether private entities may qualify as competent authorities under the LED is subject to a dedicated analysis below in Section 3.1.1.2 et seq.

[63] *See e.g.,* 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 Infrastructure Security* (Cambridge: Intersentia, 2019), pp. 27-62, 48-57.

[64] F. Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive' (2020) 11 *New Journal of European Criminal Law,* 3, 351-374, 363-374; M. Brewczyńska, 'Financial Intelligence Units: Reflections on the applicable data protection legal framework' (2021) 43 *Computer Law & Security Review*, 1-14, 11-13.

minor offences, administrative offences, or all types of offences – and thus far beyond 'criminal offences' strictly speaking.[65] In daily practice, and even where only public authorities are involved, it may prove difficult to cleanly settle which regime applies in certain scenarios: consider police officers (a LED 'competent authority') processing personal data for identification or verification purposes in the field of migration and border control (which are not 'LED purposes').[66]

Turning to data subject rights under the LED, from the point of view of both criminal investigators and the defence, it is perhaps the discrepancy between the 'right to information' enshrined in Article 14 of the GDPR and the 'information to be made available or given to the data subject' in Article 13 of the LED which most stands out. The latter provision includes two tiers of information: more general information[67] which is to be *made available* (hence: a static notice on a webpage will suffice) to the data subject, and 'further information to enable the exercise of his or her rights': (a) the legal basis for the processing; (b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period; (c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations; (d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject'.[68]

Whilst the level of prescriptiveness is low, this is a suite of information that the average criminal defence[69] would gladly seize upon in order to prepare its strategy. However, the LED permits Member States to adopt legislative measures delaying, restricting or omitting the provision of the second tier of information to the data subject in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.[70]

The scope for restrictions is thus potentially very broad, but importantly, even where Member States choose to limit the information provided to data subjects under Article 13(3), the LED introduces a duty on Member States to ensure that certain data subject rights, including that in Article 13(2), can be indirectly exercised by DPAs.[71]

---

[65] Quintel and Sajfert, 'Data Protection Directive (EU) 2016/680', 3-4. *See e.g.,* LED, Recital 13: 'A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union'. The Commission recently expressed the view that LED, Recital 13 'entails, among other things, that Member State law cannot determine the nature of an offence as being 'criminal' for the sole purpose of applying the LED'. *See,* European Commission, First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (LED) (COM LED Report), [2022] COM(2022) 364 final, 25 July 2022 , p.11.

[66] T. Quintel, 'Data Protection Rights for Third Country Nationals? Harmonization Prospects under EU Data Protection Reform', PhD thesis, University of Luxembourg, (2021).

[67] Identity and contact details of the controller, contact details of data protection officer, where applicable, intended purposes of data processing, right to lodge a complaint with a supervisory authority and contact details of that authority, existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject (LED, Art. 13(1)(a)-(e)).

[68] LED, Art. 13(2).

[69] Without forgetting convicts, victims, and (expert) witnesses, the focus here is primarily on investigator and target: the suspect, accused or defendant.

[70] To the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned; LED, Art. 13(3).

[71] LED, Art. 17. Questioning whether indirect access fulfils the main purposes of the right of access, *see further*, D. Dimitrova and P. De Hert, 'The Right of Access Under the Police Directive: Small Steps Forward', in M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer and N. Tsouroulas (eds.), *Privacy Technologies and Policy: 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers* (Cham: Springer, 2018) p. 111-130, 123-124.

For the reasons evoked in this sub-section, to mention only a few, the Commission's first report on the evaluation and review of the LED, due on 6 May 2022,[72] was keenly awaited. Following the implementation deadline of 6 May 2018, a total of nineteen Member States had faced infringement proceedings for non-transposition; by July 2019, three Member States faced actions[73] and in 2022 fresh proceedings for incomplete or inadequate implementation were launched against four Member States.[74] The Commission report was eventually released in July 2022,[75] finding that whilst on the whole national laws 'largely reflect the LED's principles and core provisions', a large number of outstanding issues remain, including both the delineation of the scope of the LED and the GDPR and data subject rights.[76]

In those respects and more, the (first) report on the LED is however of limited value in that – unlike the customary style of an evaluation report – it does not provide a full breakdown (by provision in the Directive, by country and/or by regulatory option triggered) of the national implementations.

This can admittedly be partly explained by the diversity of approaches taken at national level: whilst in several Member States the LED has been implemented in the same legal act as the GDPR (and in many instances national laws transpose the LED by referring to the same or equivalent provision of the GDPR) a number of the LED's provisions have also been transposed through new provisions in, for instance, general administrative law, administrative procedural law, or criminal procedure. Furthermore, some Member States have transposed a number of the LED's provisions in sectoral legislation regulating the operation and powers of specific competent authorities (for example, police law). 'A variety of national legal acts', the Commission concludes, 'may therefore have to be considered when determining whether or not the LED has been correctly transposed in a particular Member State'.[77]

Notwithstanding these brakes on comparability, it is regrettable that a more thorough overview has not been provided: for present purposes, little can be gleaned from the report's general observations on the LED's scope of application as enshrined in national implementing laws.[78] As concerns data subject rights, the Commission reports that all Member States have chosen to make use of the possibility in Article 15(1) LED to restrict data subjects' right of access – but stops short of providing an overview of those restrictions. 'Most' Member States reportedly also provide for restrictions of information to be made available or given to the data subject under Article 13 (discussed above) and/or the right to rectification or erasure of personal data and restriction of processing in Article 16 LED. The report continues:

---

[72] LED, Art. 62.

[73] T. Wahl, 'Infringement Proceedings for not Having Transposed EU Data Protection Directive', *Eucrim*, 10 September 2019, available at: eucrim.eu/news/infringement-proceedings-not-having-transposed-eu-data-protection-directive/. *See e.g.,* Case C-658/19, *European Commission v Kingdom of Spain* [2021] ECLI:EU:C:2021:138. Spain was ordered to pay a lump sum of €15 million plus a daily penalty payment of €89,000 for each day from the day of the judgment onward (provided the infringement still obtains) until it has put an end to the infringement.

[74] In April 2022: Finland and Sweden – both lack of access to effective judicial remedy for data subjects (respectively INFR(2022)4010 and INFR(2022)2022); Germany – gaps in transposition of the LED in relation to German Federal Police (INFR(2022)2019); Greece – non-conformity of implementing legislation on a number of points (INFR(2022)2021). In May 2022: Germany – several national laws fail to provide effective corrective powers at federal and *Länder* level (INFR(2022)2030).

[75] COM LED Report.

[76] Other priority areas, in the Commission's view, are the following: governance and powers of DPAs, remedies, time limits for storage and review of personal data, legal basis for processing, including special categories of personal data, automated decision-making, distinction between categories of data subjects, distinction between classes of personal data and verification of its quality, and logging. *See,* COM LED Report, pp. 9-16.

[77] COM LED Report, p. 9.

[78] 'Some Member States consider that a number of administrative bodies (e.g. FIUs) carry out tasks falling under the LED'; '(a) few Member States have also provided a derogation for processing by certain types of competent authorities or certain types of data'; 'some national transposing laws refer to purposes for processing personal data that are not listed in Article 1 LED (e.g. threats to public order or public safety)'. *See,* COM LED Report, p. 11.

> 'The national data protection acts transposing the LED often only follow the general language of the LED without further specifying the circumstances or the conditions in which the restrictions are to apply. In such cases, these circumstances and conditions have to be specified in sectoral legislation otherwise it would give data controllers discretion in applying these restrictions.'[79]

The lack of detail on national implementations of *inter alia* data subject rights provided by the LED is not only relevant to gauging the success of that Directive as a harmonisation measure but also makes it more difficult to discern the data protection basis upon which new direct cooperation tools such as the proposed e-Evidence Regulation would operate.

The key data protection provision in the draft e-Evidence Regulation, corresponding to Article 13 of the LED, is undoubtedly Article 11 on 'Confidentiality and user information'.[80] And whilst in principle nothing would appear to stop the e-Evidence reform bringing in tighter standards on notifying data subjects who have been targeted by a European Production Order or European Preservation Order, the potential ramifications for national levels of protection remain difficult to map without a clearer picture of implementation of the LED. We return to the contested incorporation of notification of data subjects in the e-Evidence package below in Section 4.1.2, after exploring how EU data protection law deals with public-private cooperation on digital evidence in the following Section.

3. EU data protection and public-private cooperation on digital evidence

During the gestation period of the GDPR and LED, efforts had been made by the European Parliament rapporteurs on both files to explicitly address the conundrum of public-private data processing arrangements which will inevitably engage both instruments. To this end, Jan Philipp Albrecht (GDPR rapporteur) had proposed to exclude from the scope of the Regulation data processing 'by competent *public* authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties', thereby opening the possibility that it could apply to non-public actors when processing personal data for one of those same purposes.[81] Meanwhile, Dimitrios Droutsas (LED rapporteur) proposed the insertion of a new article into the Directive capable of encompassing private-to-public data flows (termed 'access to data initially processed for purposes other than those referred to in Article 1(1)').[82]

Ultimately, in the final texts any binding provision on the data protection implications of public-private cooperation in law enforcement was conspicuously absent. This raises the question of which regime should apply to what aspects of interactions between public and private actors in the law enforcement space. In the ensuing sections, that question is explored using two essential pieces of the basic 'grammar' of EU data protection law: data controller and data processor.

The data controller is defined as 'the natural or legal person, public authority, agency or other body' (GDPR) or the 'competent authority' (LED) 'which, alone or jointly with others, determines the purposes and means of the processing of personal data'.[83] The data processor, meanwhile, is defined identically in both instruments: ''processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.[84]

[79] COM LED Report, p. 15.
[80] G. Robinson, 'The European Commission's e-Evidence Proposal' (2018) 4 *European Data Protection Law Review*, 3, 350.
[81] LIBE Committee, Draft Report on GDPR proposal, 17 December 2012, Amendment 80, p. 62 (emphasis added).
[82] LIBE Committee, Draft Report on LED proposal, 20 December 2012, new Art. 4a, Amendment 58, pp. 39-40.
[83] GDPR, Art. 4(7); LED, Art. 3(8).
[84] GDPR, Art. 4(8); LED, Art. 3(9).

Three starting points can be distinguished in the context of direct cooperation on digital evidence: public-private cooperation under the LED only, instances of public-private cooperation which engage both the LED and the GDPR, and the matter of the informal direct cooperation in light of the GDPR. The following sub-sections analyse each of these scenarios in turn through the lens of the two above-cited pieces of EU data protection law grammar: data controller and data processor.

3.1. Public-private cooperation under the LED

3.1.1. 'Delegation'

Public LED controller – Private LED processor

The most straightforward scenario of public-private cooperation involving digital evidence is that of controller and processor under the LED. Typical examples might be a forensic lab carrying out expert analysis of evidence in criminal proceedings on assignment of a court, prosecutor, or the police,[85] and a cloud service provider contracted to store a court's digital archives.[86] Such arrangements are characterised by a lack of agency for the processor, who acts 'on behalf of' the controller, in principle following without deviation the controller's instructions.

The onus is on Member States to ensure that LED controllers use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the LED, and to ensure the protection of the rights of the data subject – although the weight of the latter criterion is reduced by the requirement in Article 22(3)(b) of the LED that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The controller is thus in sole charge of whether to inform the data subject of the processing of their data, in accordance with the national implementation of the LED data subject rights regime, discussed at Section 2.2. above.

Member States shall also provide for the processing by a processor to be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[87]

This scenario (*Public LED controller – Private LED processor*) applies most cleanly to situations where data processing takes place solely on the basis of a contract containing crystal-clear instructions. To return to the example of a forensics lab, usually the very first contact such a lab will have with the material to be analysed will be governed by the contract with the controller. The very first processing of the relevant data therefore also takes place as a direct consequence of the contractual arrangement – as should, if all goes to plan, all subsequent processing until the end of the arrangement.

---

[85] T. Gottschalk, 'The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement' (2020) 1 *European Data Protection Law* 34.

[86] N. Purtova, 'Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships' (2018) 8 *International Data Privacy Law*, 1, 64.

[87] LED, Art. 22(3) further provides: 'That contract or other legal act shall stipulate, in particular, that the processor: (a) acts only on instructions from the controller; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights; (d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data; (e) makes available to the controller all information necessary to demonstrate compliance with this Article; (f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor'.

However, should such a processor at any stage determine the purposes and the means of processing, that processing can no longer be deemed to be performed 'on behalf of' the controller. As a result, the processor infringes the LED and is considered to be a controller in respect of that processing.[88] The precise contours of 'on behalf of' will vary depending on the circumstances, and it is no doubt unreasonable to demand that all technical minutiae of outsourced expert analysis be set out in advance in a contract.

In many cases, the reason a law enforcement authority requires the services of external data processors in the first place is that the public authorities are unable to do something themselves – for instance, 'brute force' a seized digital device using a proprietary technique that investigators are unable to acquire for (regular) in-house use. In such situations, the controller's instructions 'may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means',[89] but any independent determination by the processor of the purposes or the means of the processing risks triggering controllership. A case-by-case analysis remains necessary, confirms the EDPB, 'in order to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing'.[90]

In order to avoid risking a violation of the LED by a processor exceeding its remit, as clear a contract as possible is thus advisable. But contracts are not the only means by which a controller-processor relationship may be established under the LED: any 'legal act under Union or Member State law that is binding on the processor with regard to the controller'[91] may potentially suffice, thus going beyond consensual agreements to cover the imposition of LED processor status.

The *Public LED controller – Private LED processor* scenario becomes more complex, above all for the private entity and data subject, in situations where an LED processor must combine this contractual role under the LED with processing the same data under the GDPR for other purposes (typically, commercial ones). Interactions between the GDPR and LED in this kind of situation are analysed in detail in Section 3.2, after a second scenario more cleanly confined to the LED alone is addressed in the following subsection.

3.1.2. 'Private competent authorities'

Public LED controller – Private LED controller

The foregoing section showed that if an LED processor crosses a certain threshold of agency, it may de facto become an LED controller 'by accident'. But the Directive also opens the space for a private entity to become a data controller under the LED by design – when it is appointed as a private 'competent authority'. As noted above, in Article 3(7) of the LED one finds a two-fold definition of 'competent authority': any public authority competent for Article 1(1) purposes, or 'any other body or entity entrusted by Member State law to exercise public authority and public powers' for those same purposes.[92]

---

[88] As provided by LED, Art. 22(5), mirroring GDPR, Art. 28(10).

[89] European Data Protection Board (EDPB) 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0', 7 July 2021, para. 80, p. 26. As the Commission recently noted, whilst LED, Art. 51 sets out the EDPB's tasks in relation to processing within the scope of the Directive, '(m)any of the EDPB's guidelines on the GDPR are also relevant for the LED to the extent that they rely on common concepts or technologies. Such guidelines include those on the concept of data controller and processor (…)'. *See,* COM LED Report, p.24.

[90] EDPB, 'Guidelines 07/20', para. 82, p. 27.

[91] *See,* LED, Art. 22(3) and the stipulations therein as to the minimum contents of the contract or other legal act. Comparing data processor status to delegation, *see also,* EDPB, 'Guidelines 07/20', para. 80, p. 26.

[92] Only the public limb of this definition had been included in the Commission proposal from 2012 (Art. 3(14)), with the second limb – added during negotiations – opening up the potential for application of the LED to private actors.

In its July 2022 report on the 'application and functioning' of the LED, the Commission shared its view that 'competent authorities' as defined by the LED are:

> 'either organs of the State or private bodies, on which the law confers special powers beyond those which result from the normal rules applicable in relations between individuals and/or by the possibility of exercising the power of coercion. These authorities are competent authorities under the LED when (even if only sporadically and/or in isolated cases) they process data for the purpose of preventing, investigating, detecting or prosecuting criminal offences or of executing criminal penalties (including safeguarding against and preventing threats to public security).'[93]

Regarding the national implementations, the Commission reported:

> 'Most of the Member States' laws comprehensively cover any competent authority processing of data for LED purposes. By contrast, some Member States have chosen to exhaustively enumerate the competent authorities under the LED in their national legislation. A few Member States have also provided a derogation for processing by certain types of competent authorities or certain types of data.'

Regrettably, no further information is shared on whether, which and how Member States have used the possibility to allow for 'private competent authorities' in national laws. However, the emerging literature would seem to confirm that at least some Member States have taken up this option. For example, through a combined reading of national legislation and DPA guidance in six Member States, Vogiatzoglou and Fantin have placed the Republic of Ireland, Italy and France (together with ex-Member State the United Kingdom) into that camp.[94]

For all of the EU-27 which have done likewise, it will be instructive to make out the precise contours in national law of the phrase 'entrusted by Member State law to exercise public authority and public powers' for LED purposes. It was noted earlier[95] how Recital 12 of the Directive has led to a broadening of the scope of *public* competent authorities in certain implementations. In relation to *private* competent authorities, a thorough comparative view would take in the following aspects for each jurisdiction: how *private* competent authorities may be designated 'by Member State law' (primary or secondary legislation, law or decree, closed list or case-by-case designations?); exactly what public authority and/or powers may be entrusted to them as data controllers;[96] and the identity and tasks of private entities currently thus designated in each Member State.

Whilst the wording 'entrusted' by law to exercise public authority and public powers (and *a fortiori,* for instance, the wording 'authorised' in the Irish act implementing the LED[97]) might suggest a limitation to private entities which willingly take on the role of private competent authority (for example, a company joining a public-private-partnership (PPP) to combat cybercrime),[98] it seems likely that a private entity may be made an LED competent authority by law without its having sought such a role: for instance, 'critical infrastructures' identified in the framework of EU legislation.[99] Yet other entities may be difficult to categorise as either

[93] COM LED Report, p. 10.
[94] Vogiatzoglou and Fantin, 'National and Public Security', pp. 51-57.
[95] In Section 2.2.
[96] Purtova remarks, furthermore: 'It appears that it is possible for such a private party to be seen as a competent authority for the purposes of the Directive even when the national law does not formally recognize it as a law enforcement authority, but grants public authority and public powers for the law enforcement purposes in Article 1(1) (LED)'; 'Between the GDPR and the Police Directive', 66. All the same, and as she also notes (at 65-66), Art. 3(8) LED states that 'where the purposes and means of (processing by a competent authority) are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'. This provision mirrors Art. 4(7) of the GDPR.
[97] Data Protection Act 2018, S. 69(1)(b).
[98] Purtova, 'Between the GDPR and the Police Directive', 52.
[99] *See,* Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, [2008] OJ L 245, 23 December 2008, p. 75-82. Given the 'body or entity' wording in the LED, the private competent authority would

public or private: for instance, a state-owned public transport company, put in charge by national law of handling ticket offences.

For the fruits of a private competent authority's data processing to be used by a public competent authority, and inherently so for digital evidence, some form of data transfer between a private competent authority and a public competent authority will usually be required. In such circumstances, 'where two or more controllers jointly determine the purposes and means of processing', Member States are bound by Article 21 LED to provide for them to be joint controllers. They shall, moreover:

> '(…) in a transparent manner, determine their respective responsibilities for compliance with (the LED), in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13,[100] by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate the contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.'

Dividing up responsibilities between joint LED controllers will be more straightforward when the data in question is processed exclusively for LED purposes: for instance, a privately-run prison under contract with the national prison service to process inmates' personal data. Such a private competent authority will still have to juggle its role as an LED controller for prisoner data with parallel responsibilities under the GDPR in relation to other personal data – for instance, staff data for HR purposes[101] – but a clear demarcation between legal regimes is in place, laying the foundation for the assignment of respective roles by contract or other legal act.

Matters become less clear-cut whenever the *same data* is processed by a private processor (tackled in the preceding section) or a private joint controller (as just discussed) under the LED for its purposes as well as under the GDPR for other purposes. An example that could fit either scenario – to the extent that personal data is in play – is a private entity performing blockchain analytics both for commercial market analysis and to assist cryptocurrency-related investigations.[102]

Taking private LED *processors* first, Recital 11 restates that 'the application of (the GDPR) remains unaffected for the processing of personal data outside the scope of this Directive'. Of itself, this does not provide a conclusive answer to the 'two hats' conundrum identified in the literature: a private actor processing personal data as an LED processor on behalf of an LED controller is bound to confidentiality under that legal instrument,[103] but must *also* comply with data subject rights under the GDPR – in this case Articles 13 and 14 GDPR. Without a clear

be the 'European critical infrastructure' (ECI) itself, rather than its owner/operator or Security Liaison Officer. This example is also put forward by Vogliatzoglou and Fantin, 'National and Public Security', p. 50.

[100] Discussed in Section 2.2. above.

[101] Similarly to public authorities processing data for different purposes, including EU institutions, bodies, offices and agencies (IBOAs) such as the European Public Prosecutor's Office (EPPO) with two different data protection regimes for operational and administrative personal data. *See e.g.,* V. Franssen and M. Corhay, 'Interpretation of the EPPO Regulation in view of EPPO's supervision by the EDPS', *European Data Protection Supervisor*, 12 April 2021, available at: https://edps.europa.eu/data-protection/our-work/publications/reports/interpretation-eppo-regulation-view-eppos-supervision_en.

[102] For example, Chainalysis. *See e.g.,* M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert and P. Pesch, 'Safeguarding the evidential value of forensic cryptocurrency investigations' (2020) 33 *Forensic Science International: Digital Investigation*, 1-14. '(W)here forensic analyses are outsourced and conducted by (private) third parties (…), the GDPR can remain applicable'.

[103] LED, Art. 22(3)(b).

selection of legal regime in law,[104] the dual application of both regimes is thus liable to give rise to dual, conflicting obligations.[105]

Turning to the second scenario, private competent authorities acting as *joint controllers* under the LED will often simultaneously handle the same personal data under the GDPR, for other purposes. This situation mirrors that of a public competent authority (for example, police, prosecutor or judge) which must apply either the LED for processing pertaining to their core functions or the GDPR for any other purpose. It also immediately throws up a host of questions as to how several provisions of the LED could be applied by private controllers, whether regarding key data processing principles[106] or data subject rights – especially where comparable duties exist in the GDPR in relation to the very same data.[107] In any case, as seen above, a private competent authority must be entrusted with public authority and public powers by Member State law – providing an opportunity to ensure much-needed clarity on respective responsibilities from the start of joint processing operations.

At the EU level, the Commission's direct cooperation mechanism as envisaged in the initial e-Evidence package would appear to neatly fit the LED joint controllership provisions in several core respects: there is processing of data for LED purposes, with the exercise of public authority and powers entrusted to a private entity, and the means of processing at least co-determined by that private entity – a fortiori where production orders must be assessed for manifest violation of fundamental rights and/or abuse.[108]

Whilst both the EU Council and the European Parliament subsequently excised that particular test from their starting positions for trilogues, instances wherein application of the LED instead of the GDPR cannot be discounted so long as the e-Evidence Regulation limits itself to mentioning that the two instruments apply as an *acquis.* As Corhay has opined, '[o]ne can regret that, so far, the EU institutions have missed the opportunity to adopt a position on some important questions such as the instrument – the GDPR or the LED – that must apply when public authorities access data stored by private actors'.[109] The risks attached to overlapping legal regimes are further unpacked in the following sub-section.

3.2. Public-private cooperation, the LED and the GDPR

Public LED Controller – Private GDPR Controller

Having reiterated the space created in Article 3(7) LED for the appointment of non-public bodies or entities as competent authorities under this Directive, Recital 11 LED begins to address the attendant risk of overlapping EU data protection regimes as follows:

---

[104] Or a clear restriction of the scope of application of the GDPR under Art. 23; given this chapter's focus on digital evidence in criminal matters, such a restriction would be based on Art. 23(1)(d) GDPR.

[105] Purtova, 'Between the GDPR and the Police Directive', 65-66. The point has also been raised within the *Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680*, citing the example of a law enforcement authority engaging a private company as a processor in order to decrypt a hard disk for investigation purposes. For some members, '(s)uch situations raised difficulties in application of different legal regimes to the same data sets, in particular as regards data subject rights. The Commission suggested that national laws could lay down the rules on joint controllership and responsibility for the personal data in such databases, as well as the rules on the point of contact for data subjects (conversely Art. 26(1) GDPR).' *See,* Minutes of the fifteenth meeting of that expert group, 20 February 2018, available at: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=3656&fromExpertGroups=true.

[106] For instance, the distinction between different categories of data subject as required by LED, Art. 6 or the duty in LED, Art. 7(1) to distinguish personal data based on facts from personal data based on personal assessment.

[107] Compare for instance LED, Art. 16 (on the right to rectification or erasure of personal data and restriction of processing) with GDPR, Arts. 16-20.

[108] Decried by Mitsilegas as a de facto 'privatisation of mutual trust'. *See,* V. Mitsilegas, 'The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of e-Evidence' (2018) 25 *Maastricht Journal of European and Comparative Law*, 3, 263.

[109] M. Corhay 'Private Life, Personal Data Protection and the Role of Service Providers' (2021) 6 *European Papers*, 1, 471.

> 'Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law.'

Reflecting the fact that the two instruments together formed a package, the first sentence mirrors the carve-out in Article 2(2)(d) of the GDPR, in its final form without the Albrecht amendment mentioned above.[110] The first clause in the second sentence also merely restates the *lex generalis* baseline: where a body or entity collects personal data for "other purposes" (i.e. non-LED purposes), the GDPR should apply.[111] So far, so consistent.

The second clause of the second sentence then ostensibly refers to Article 6(1)(c) of the GDPR, establishing a legal basis for data processing where 'necessary for compliance with a legal obligation to which the controller is subject'. Yet this is not the same as asserting that *only* the GDPR may apply to such further processing – for instance, where digital evidence is transferred to a public LED data controller. In other words, on a literal reading the eventuality that a private entity may act simultaneously as GDPR controller and LED joint controller in relation to (at least) a transfer of data between cooperating entities is not discounted.

On this view, the transfer of digital evidence between private actor and public authority would no longer fall between the cracks of the EU data protection legal framework, as the consensus in doctrine had it before the 2016 reforms,[112] but be subject to a mild form of hyperregulation: the *lex specialis* (carrying lower standards of protection) can apply on top of the *lex generalis* (carrying higher standards of protection).

Furthermore, the lack of any ascription of data controllership in Recital 11 also generates uncertainty: when a private actor, in compliance with a legal obligation upon it, transfers digital evidence to investigators, where does controllership arise? Joint controllership is a possibility under the LED, but even where this does not obtain (for instance, where the private actor is not on a closed list of LED competent authorities determined in national law) and the GDPR alone applies, is joint controllership under the GDPR conceivable?

It might seem counterintuitive to consider that an entity which is constrained by a legal obligation can be labelled a *controller*, but this is the position taken by Purtova, one of (very) few scholars to have traced in detail what she calls the 'maze' of information sharing in public-private-partnerships in light of both the GDPR and the LED.[113] Whilst there will be many scenarios in which the GDPR controller's decisional agency is reduced to virtually zero (for instance, where a prosecutor orders production of specific subscriber data behind a defined IP address),[114] in Purtova's view, even when it is under a legal obligation to 'further process' data, a certain degree of control always remains with the initial controller under the GDPR: 'the private party should assess if the processing is necessary and proportionate to satisfy the legal obligation at hand, how much and which data is necessary and sufficient, whether

[110] 'This Regulation does not apply to the processing of personal data: (…) (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.

[111] 'Should' apply since the breadth of this assertion ("other purposes") is already open to question on the grounds that the GDPR does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, pursuant to Art. 2(2)(a) of the GDPR. The Regulation, although of *general* application, was never designed to cover processing for *all* possible purposes. *See,* M.-E. Ancel, 'D'une diversité à l'autre. A propos de la « marge de manœuvre » laissée par le règlement général sur la protection des données aux États membres de l'Union européenne' (2019) 2019 *Revue critique de droit international privé,* 3*,* 647.

[112] G. Boulet and P. De Hert, 'Cooperation between the private sector and law enforcement agencies: an area in between legal regulations', in H. Aden (ed.), *Police Cooperation in the European Union under the Treaty of Lisbon. Opportunities and limitations* (Baden-Baden: Nomos, 2015), pp. 245-258.

[113] Purtova, 'Between the GDPR and the Police Directive', 52.

[114] As Purtova indeed identifies. *See,* 'Between the GDPR and the Police Directive', 64.

providing for anonymous data would suffice or identifiable data is necessary, etc'.[115] This in turn connects to an ongoing debate within EU data protection law and policy, well away from the world of cross-border criminal investigations (and rather too distant to cover in depth here), surrounding a fragmented conceptualisation of data controllership seemingly advocated by the CJEU in *Fashion ID*.[116]

For present purposes, it suffices to illustrate one important related unclarity emerging from jurisprudence closer to home: the aforementioned twin judgments in *Privacy International* and *La Quadrature du Net.* As seen in Section 2.1., it was the extension of *effet utile* reasoning (previously employed by the Court in relation to national data retention legislation measures for the combatting of crime) to data retention for national security purposes, thus pulling the latter within the scope of EU law – and the inevitable thorough proportionality assessment – which has garnered most attention[117] and triggered diverse responses in the Member States[118] as well as a confrontational ePrivacy Regulation mandate from the Council.

In *Privacy International* and *La Quadrature du Net,* the Court's assignation of legal regimes turns on personal scope: wherever data processing obligations are imposed on providers of ECS, whether to safeguard national security or combat crime, the ePrivacy Directive applies to that processing.[119] By contrast, where Member States 'directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of [ECS], the protection of the data of the persons concerned is covered not by the ePrivacy Directive, but by national law only, subject to the application of the [LED] (…)'.[120]

Viewed through this chapter's prism of public-private cooperation on digital evidence, at least three questions are left on the table by the Court's *clivage* in *Privacy International* and *La Quadrature du Net.*

The first question is linked to what the Court does *not* state: that where ECS providers process data for the safeguarding of national security or the combatting of crime pursuant to a legal obligation, *only* the ePrivacy Directive applies. Indeed, as the ePrivacy Directive is much less detailed than the GDPR, ECS providers will need to rely on the latter instrument wherever the former instrument has not 'supplemented and specified' it[121] – for instance, to ascertain obligations with regard to data processing principles and data subject rights. At the same time, application of the LED is not excluded by the Court.

Secondly, does the ECS provider act as a data processor or a (joint) controller, and under which instrument(s)? The Court does not provide concrete guidance in this regard, beyond a construal of Articles 23(1)(d) and (h) GDPR to observe that 'the processing of personal data carried out by individuals for those same purposes falls within the scope of that Regulation'.[122] There is an echo here of the Court's *effet utile* reasoning with regard to the scope of Article

[115] Purtova, 'Between the GDPR and the Police Directive', 64.

[116] Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629. *See,* M. Zalnieriute and G. Churches, 'When a 'Like' Is Not a 'Like': A New Fragmented Approach to Data Controllership' (2020) 83 *The Modern Law Review,* 4, 861-876; M. Finck, 'Cobwebs of control: the two imaginations of the data controller in EU law' (2021) 11 *International Data Privacy Law,* 4, 333-347.

[117] Pointing out a viable alternative interpretation of the relevant provisions in the ePrivacy Directive. *See,* Iain Cameron, 'Metadata retention and national security: *Privacy International* and *La Quadrature du Net*' (2021) 58 *Common Market Law Review* 1458. For criticism of the reasoning used by the Court to distinguish away its earlier decision in *PNR* (Joined Cases C-317/04 and C-318/04, *Parliament v. Council and Commission* [2006] ECLI:EU:C:2006:346). *See,* Tzanou and Karyda, 'One Step Forward Two Steps Back',128-129.

[118] S. Vallée and G. Genevoix, 'A Securitarian Solange. France has launched a cluster bomb on the EU's legal and political order', *Verfassungsblog,* 25 April 2021, available at: https://verfassungsblog.de/a-securitarian-solange/; Cécile de Terwangne, 'L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de Justice de l'Union Européenne' (2022) 129 *Revue trimestrielle des droits de l'homme* 3-27.

[119] *Privacy International*, para. 46*; La Quadrature du Net*, para. 101.

[120] *Privacy International,* para. 48; *La Quadrature du Net,* para. 103.

[121] *Privacy International,* para. 47; *La Quadrature du Net,* para. 102.

[122] *Privacy International,* para. 46*; La Quadrature du Net*, para. 102.

15(1) ePrivacy Directive: in essence, if there is a limitation clause, that which may be limited by such a clause must fall within the scope of the instrument. Yet it is the use of the word 'individuals', which does not appear in the cited provisions of the GDPR, which puzzles. Although the cited passage of the judgments is doubtless obiter, might the Court be offering, *sotto voce*, space now to accommodate 'private competent authorities' under the LED, and/or room to manoeuvre in future for a fragmented notion of data controllership?

The answer matters since the bifurcated edifice of the EU data protection *acquis* is fundamentally challenged by data processing which shifts between 'public' and 'private' realms, whether in isolated instances or in the course of more stable partnership-like arrangements, inherently engaging both GDPR and LED. Most evidently, the purpose limitation principle enshrined in Article 5(1)(b)[123] GDPR risks being effectively emptied should data handled by private service providers 'slip' from the ambit of the GDPR to the prosecutor, judge, police or other competent authority, operating (for core purposes) under the LED.[124]

The average EU citizen, unversed in the highly legalistic nature of the data protection discussion, is well entitled to wonder: how can the second processing purpose *not* be 'incompatible' with the first?[125] Furthermore, once data is transferred to the competent authority side, the suppler LED rules kick in: in particular, unlike the Regulation,[126] the Directive does not contain the concept of 'further processing'. Subsequent processing by the same or a different competent authority is allowed for other LED purposes, if this is provided for by law, necessary and proportionate.[127]

The obvious (and perhaps only) reply is that the incompatibility of such secondary use is exceptionally justified by the needs of law enforcement to obtain the personal data in order to perform their tasks. Investigative needs, simply put, trump purpose limitation. To borrow the conceptual lens of De Hert and Gutwirth, the 'channelling' function of data protection law is here much more present than its 'blocking' function.[128] Yet when the free movement of data – the 'forgotten twin' objective of EU data protection law[129] – wins out and once purpose limitation is foregone in the re-use of privately-gathered data for the public purposes of law enforcement – what then remains of that channelling function? If the immediate rejoinder is

[123] 'Personal data shall be: (…) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')'.

[124] LED, Art. 4(1)(b) includes the purpose limitation principle, but this is limited to the collection of data under the LED. In most private-to-public scenarios, data will initially have been collected under the GDPR.

[125] *See further,* Article 29 Working Party, Opinion 03/2013, pp. 23-27, and C. Jasserand, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation' (2018) 2 *European Data Protection Law Review* 152–167. Along similar lines, *see,* Advocate General Szpunar's observation, in para 131 of his Opinion in *Penalty Points,* that 'private companies might be tempted to exploit personal data for commercial purposes, that is to say, for purposes that are incompatible with the purpose of the processing, which is to increase road safety'. *See,* Opinion of Advocate General Szpunar in Case C-439/19 *B v Latvijas Republikas Saeima (Penalty Points),* [2020] ECLI:EU:C:2020:1054.

[126] *See e.g.,* GDPR, Recital 50, also discussed in Section 3.3.

[127] LED, Art. 4(2). *See further,* Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7 November 2016, available at: https://ec.europa.eu/transparency/expert-groups-register/core/api/front/expertGroupAddtitionalInfo/27802/download. Of course, in contrast to the GDPR, in the law enforcement context the consent of the data subject cannot be a ground for data processing. *See e.g.,* LED, Recital 35.

[128] For the cited authors, the blocking function of data protection law renders the individual opaque to public power and corresponds to *privacy*, in contra-distinction to its channelling function, which accepts that the data subject is rendered transparent to public power, in return for the constraining and reciprocal transparency of use of that power: appropriately-circumscribed data processing principles, meaningful data subject rights, and effective independent supervision. *See,* P. De Hert and S. Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', in E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the criminal law* (Antwerp/Oxford: Intersentia, 2006), pp. 61-104.

[129] TFEU, Art. 16; GDPR, Art. 1(1).

'data subject rights and independent supervision', effective fulfilment of the latter can only be hampered by such levels of indeterminacy as regards the applicable legal regime(s).

Returning to the questions left on the table post-*Privacy International* and *La Quadrature du Net*, the third pertains to the space in between the two poles distinguished by the Court and marks the way to the final part of Section 3. In distinguishing the obligation to retain data and the relevant provisions on accessing that data (which *do* fall within the scope of the ePrivacy Directive for the purposes of the Court's fundamental rights check) from the 'direct implementation' of data processing measures by public authorities (which escapes that check, and is subject to national law *only*), the judgments remain silent on voluntary cooperation. Now, it seems logical to surmise that an absence of clarity in the data protection parameters of formal public-private cooperation on digital evidence has contributed to (or even arguably sustained[130]) the growth of informal 'voluntary' cooperation between ECS and law enforcement both domestically and transnationally. The following sub-section examines this last scenario in more detail.

Before proceeding to voluntary cooperation, however, it is worth underlining that the studied case law 'only' concerns ePrivacy Directive *regulatees* – which already covers a lot of digital evidence, but far from every source. It is also indelibly linked to that legal instrument, in the sense that the priorities and vision of the EU legislator calibrated at the turn of the millennium, as expressed in the Directive's articles and recitals, drives much of the Court's argumentation – in terms of normative load-balancing as well as interpretation of black-letter law. In months and years to come, it will be imperative to track the extent to which the incoming ePrivacy Regulation reflects and respects the Court's positioning so far, and influences it thereafter.[131]

3.3. Informal direct cooperation and the GDPR

Public LED Controller – Private GDPR Controller

In the here and now, the consensus seems to have it that most cooperation between internet service providers and law enforcement is taking place on an 'informal' or voluntary basis – voluntary in the sense that the service provider's local law (i.e. where the service provider is headquartered or represented) does not explicitly recognise an 'order' or request from foreign law enforcement as legally binding. Local law often also positively prohibits compliance with a foreign-origin request – as exemplified in a transatlantic setting by the so-called '*Microsoft Ireland'* litigation,[132] and within the EU by the *Skype* case.[133] In such cases, any cooperation afforded will be voluntary – but it will also represent in principle a (conscious) violation of local law and risk attracting the relevant sanctions.

In most EU jurisdictions, as in *Skype* (at the time, headquartered in Luxembourg), domestic implementations of the ePrivacy Directive prohibit the voluntary direct divulgation of user data to foreign investigators by ECS including – since the EEC reform of late 2020 – many OTT services. Where no such bar is in place, the question arises of the compatibility of informal direct cooperation with data protection law – first and foremost, the GDPR. In this chapter, the cooperation of EU-based service providers with investigators in third countries (such as the

[130] A. Aguinaldo and P. De Hert, 'European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law' (2020) 6 *Brussels Privacy Hub Working Paper* 26, 1-16, available at: https://www.brusselsprivacyhub.eu/publications/wp626.

[131] *See also,* X. Tracol, 'The joined cases of *Dwyer, SpacNet* and *VD and SR* before the European Court of Justice: The judgments of the Grand Chamber about data retention continue falling on deaf ears in Member States' (*forthcoming*, 2023) 48 *Computer Law & Security Review* 14.

[132] *See,* D. M. Sullivan, 'Brief of EU Data Protection and Privacy Scholars as Amici Curiae in Support of Respondent in United States of America v. Microsoft Corporation', 18 January 2018, available at: https://www.supremecourt.gov/DocketPDF/17/17-2/28272/20180118141249281_17-2%20BSAC%20Brief.pdf. The author was one of 21 signatories of the amicus brief.

[133] Belgian Supreme Court, 19 February 2019, P.17.1229.N.

United States) is set aside in order to focus on cooperation within the EU, with a view to complementing certain national chapters on EU Member States in this volume.

McIntyre is one of few commentators to have closely examined the legal position of internet service providers involved in informal cooperation with foreign investigators – in his case, providers based in Ireland – in terms of its compatibility with the purpose limitation principle and the legal bases for such processing which may be available in the GDPR. McIntyre determines that, save in exceptional cases such as where a provider detects fraud in relation to its own service and reports it to law enforcement, much voluntary cooperation with foreign investigators will not fulfil the five criteria set down in Article 6(4) GDPR.[134] As those criteria are non-exhaustive, a discrete analysis will be required in each instance of voluntary cooperation.

Should compatibility between one purpose and the next not obtain, the lawfulness of the processing can only be preserved by either the consent of the data subject (a non-starter in the criminal investigation context) or 'a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard' the objectives (including the combatting of crime) referred to in Article 23(1) GDPR, and also meets the cumulative requirements set down in Article 23(2). Each national system will then fall to be assessed against those requirements. In the case of Ireland, McIntyre concludes that the blanket disapplication of the purpose limitation principle in national law will generally leave voluntary disclosure in breach of that principle;[135] from a broader EU perspective, it was noted in Section 2.2. that the Commission's recent report on the implementation of the LED has shed little light on the situation across the Member States.

Turning to the matter of a suitable GDPR legal basis for the voluntary disclosure of data to foreign investigators, McIntyre notes the consensus[136] shared by the EDPS, the EDPB and in the academic literature that the only possible grounds are protection of the vital interests of a natural person[137] – connoting emergency, and as such inherently of limited application – or the legitimate interests of the data controller or a third party.[138] Recital 50 to the GDPR states that '[i]ndicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller'. But given its tenor ('*indicating* possible criminal acts'), the provision sits much more neatly with own-initiative notification of the relevant competent authority by the controller than with requests for digital evidence addressed by such an authority to service providers.[139]

Lastly, to the extent that legitimate interests can be established as a ground for processing in the context of informal cooperation on digital evidence, that ground in any case dissolves where it is overridden by the interests or fundamental rights and freedoms of the data subject

[134] In the absence of both the data subject's consent and a Union or Member State law pursuant to Article 23(1) GDPR, the controller 'shall take into account, inter alia:
1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
4. the possible consequences of the intended further processing for data subjects;
5. the existence of appropriate safeguards, which may include encryption or pseudonymisation.'

[135] McIntyre, 'Voluntary Disclosure of Data to Law Enforcement', pp. 10-11.

[136] McIntyre, 'Voluntary Disclosure of Data to Law Enforcement', p. 11 and the sources cited there, in footnotes 48 and 49.

[137] GDPR, Art. 6(1)(d).

[138] GDPR, Art. 6(1)(f).

[139] McIntyre, 'Voluntary Disclosure of Data to Law Enforcement', p. 12.

which require protection of personal data, in particular where the data subject is a child.[140] This in turn requires an individualised assessment of the need for disclosure and the impact on the data subject.[141] For McIntyre, the upshot is that service provider policy or practice of blanket voluntary disclosure to law enforcement on the basis of a request are per se unlawful.[142] For the purposes of this chapter, and not for the first time, close similarities between the implications of such an individualised assessment and the Commission's 2018 vision for the European Production and Preservation Orders, and in particular their vetting by service providers for manifest violations of Charter rights, hove into view.

4. Digital evidence reforms in the two Europes[143]

4.1. The EU e-Evidence package[144]

At first glance, the dual-instrument e-evidence package presented by the European Commission in April 2018 does not seem to have all that much to do with data protection. There is no reference to 'data protection' in the binding articles of the draft e-Evidence Regulation, and the GDPR and LED are mentioned obliquely in just one article (Article 17), which provides that 'effective remedies' under national law against European Production Orders will be available at the eventual criminal proceedings in the issuing state 'without prejudice' to data protection remedies under the *acquis*. As for the accompanying draft LRD, there is no reference to 'data protection' in its main text.

Of the draft Regulation's sixty-six (non-binding) Recitals, 'data protection', the GDPR or the LED are mentioned in seven. One is a boilerplate closing reference to prior consultation of the European Data Protection Supervisor (EDPS),[145] and another evokes requirements on national authorities and service providers to put in place suitable technical measures for the public-private direct cooperation regime, including data security.[146] Two further Recitals make a general reference to the existing EU data protection *acquis* in the context of justifying stricter controls in the mechanism on access to certain categories of data ('transactional data' and content data) than to others ('access data' and subscriber data),[147] and briefly mention service providers' liability arising from 'good faith' compliance with data orders.[148] As for the preamble to the LRD, a mere two Recitals feature the terms.[149]

The dearth of references to data protection in the legislative package can be partly explained by the two instruments' legal bases, respectively judicial cooperation and the internal market – although it does invite inquiry as to where policy priorities lie.[150] In the accompanying Impact

[140] McIntyre, 'Voluntary Disclosure of Data to Law Enforcement', p. 12.
[141] GDPR, Recital 47 and McIntyre, 'Voluntary Disclosure of Data to Law Enforcement', p. 13, citing Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate Interests of the data controller under Article 7 of Directive 95/46/EC', [2014] 844/14/EN.
[142] McIntyre, 'Voluntary Disclosure of Data to Law Enforcement', p. 13.
[143] The expression is borrowed from P. De Hert, G. González Fuster and B.-J. Koops, 'Fighting Cybercrime in the Two Europes. The added value of the EU framework decision in the Council of Europe Convention' (2006) 77 *Revue internationale de droit penal*, 3, 503-524.
[144] For a more comprehensive analysis see, in this volume, T. Christakis.
[145] Draft e-Evidence Regulation, Recital 66.
[146] Draft e-Evidence Regulation, Recital 57.
[147] Draft e-Evidence Regulation, Recital 23.
[148] Draft e-Evidence Regulation, Recital 46. The remaining two Recitals are reminders – for the co-legislators (Recital 2) and for the Member States implementing the Regulation (Recital 56) – of the status of data protection as a fundamental right.
[149] One (Recital 24) similarly provides for consultation of the EDPS, and the other (Recital 6) draws a parallel between the envisaged appointment of legal representatives for the 'receipt of, compliance with and enforcement of' (this language from Recital 7) orders to produce or preserve electronic evidence with the existing requirement to establish a legal representative for data protection matters under the GDPR.
[150] For criticism of the choice of legal basis for the draft Regulation, *inter alia* from a territorial sovereignty perspective. *See,* M. Böse, 'An assessment of the Commission's proposals on electronic evidence', *European*

Assessment,[151] one begins to see the multifaceted role played by data protection (and privacy) in the e-Evidence debate. It is possible to discern three main features.

First, as the proposal only covers electronic evidence which is already in existence (for instance, call records or message contents backed up by a tech company), the strengthening of data protection rules is recognised in the Commission's Impact Assessment as a threat to the very availability of digital evidence for investigations. In particular, as noted in Section 2.1., a comprehensive embedding of the principle of data minimisation would reduce the amount and types of data entering the 'pipe'. From an enforcement perspective, the logic of data minimisation is compounded by the continued absence of an EU-level obligation on communications service providers to retain traffic and location data.

Second, there is fragmentation: increasingly divergent data protection and privacy rules (and their application at national level) are represented in the Commission's Impact Assessment as a block in the pipeline of direct cooperation. This concern mirrors the single biggest driver of the proposal per se: the discrepancies and lack of clarity surrounding the legality of cross-border direct cooperation have already generated levels of legal uncertainty which is detrimental to law enforcement as well as service providers, and action at the EU level is required lest the national laws of more Member States shift to a generalised extraterritorial use of enforcement jurisdiction.[152]

The third and last main role played by data protection in the Commission's e-Evidence package reflects the global scene on which criminal investigations increasingly play out. Indeed, although EU law measures, the mooted European Production and Preservation Orders are inescapably extraterritorial-by-design: by proposing to retire data storage location as determiner of jurisdiction, the EU legislator is only too aware of the risks, first, of generating conflicts of law and, second, of triggering the adoption abroad of (further) reciprocal measures targeting European service providers.[153] On a broader and longer view, there is arguably also the potential for uncoordinated extensions of the 'sword' of law enforcement into the cloud to fuel a worldwide shift to data localisation and a future of fractured 'data sovereignties'.[154]

Given these friction risks, the EU legislator has included the safety net of a review procedure in case of conflicting obligations under third country law,[155] whilst in parallel the co-legislators also espouse the goal of including EU data protection norms in their external action, partly in order to ensure their fulfilment within the Union.[156] Even in the absence of any international agreement, the EU legislator aims to deliver in the e-Evidence reform 'a measure that contains strong safeguards and explicit references to the conditions and safeguards already inherent in the EU [data protection] *acquis*, thus serving as a model for foreign legislation'.[157]

Parliament, 21 September 2018, pp. 35-37, available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)604989.

[151] COM e-Evidence IA.

[152] Compare Böse, who argues that the proposed mechanism will not fully overcome the current fragmentation of divergent cooperation regimes in the Member States' criminal justice systems. See, Böse, 'An assessment of the Commission's proposals', pp. 43-45.

[153] In particular business organisations responding to the open consultation on the e-Evidence reform highlighted the need for a 'full assessment of the risks arising from reciprocal action of non-EU countries'; COM e-Evidence IA, p. 126. In this vein, *see further* in the same document p. 96, 105, 124, 127, 171.

[154] Ligeti and Robinson, 'Sword, Shield and Cloud', p. 70.

[155] *See,* Draft e-Evidence Regulation, Arts. 15-16, and in this volume T. Christakis.

[156] *See e.g.,* Press release, 'Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters', Council of the European Union, 6 June 2019, available at: https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/, and Par*t III ('Safeguards') of the e-evidence negotiating directive accessible therefrom.* See more recently, Directorate-General for Justice and Consumers, 'EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations', European Commission, 2 March 2023, available at: https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.

[157] Draft e-Evidence Regulation, p. 10.

The following sub-sections reflect on the likely impact of the e-Evidence reform on effective data protection within the EU, addressing successively the models put forward by the European Commission, the EU Council and the European Parliament, before the discussion narrows to focus on the 'gateway right' of 'information to the data subject', ie notification of the target of an investigation. A final sub-section then offers a first reaction to the final compromise text of the e-Evidence Regulation, which emerged just as this chapter was being finalised.

4.1.1. Data protection and the European Production Order

4.1.1.1. European Commission – De facto joint controllership

In the Commission model, European Production (and Preservation) Orders are addressed to the legal representative or potentially any establishment of the service provider in the Union.[158] In Section 3.1.2. above, it was argued that the 'manifest violation / abuse' control operated by service providers[159] could imply joint controllership status under the GDPR – or potentially even the LED – for those private entities.

The lack of decisive ascription of controllership in the proposals was strongly criticised by the EDPB, with the Board expressing concern that the definition of 'service provider' to mean 'any natural or legal person that provides one or more of the following categories of services'[160] in conjunction with a broad definition of 'offering services'[161] could cover both controllers and processors (for instance, processors storing data for controllers) in the sense of the GDPR.[162]

This matters above all since, by its nature, a processor acts on instructions given by the controller; it is the responsibility of the latter to ensure the rights of data subjects are respected. In concrete terms, should a *processor* (say, a storage service in Member State B) receive one of the new orders to produce or preserve digital evidence instead of a *controller* (say, the legal representative based at headquarters in Member State A), the former would not receive access requests from data subjects and will not be in a position to answer such requests unless expressly asked to do so by the latter. Meanwhile, where it is the processor who receives an order to produce or preserve digital evidence, the controller receiving access requests from the data subject may simply not have (all) the sought information. The result in practice, fears the Board, could be a de facto dilution or even circumvention of data subject rights (provided that such rights have not already been limited in Union or Member State law in full compliance with Article 23 GDPR).[163]

Both EDPB and EDPS have, more broadly, called for clarification of the roles to be played by legal representatives under the LRD and legal representatives under the GDPR, given the 'important differences in terms of role, liability and relationship with the other establishments of the service provider in one case and controller or processor in the other' – recommending that two different legal representatives should be designated, each with clear distinct functions according to the relevant instrument: e-Evidence or data protection.[164]

---

[158] Draft e-Evidence Regulation, Arts. 7(2)-(4).
[159] Draft e-Evidence Regulation, Arts. 9(5), 14(4)(f) and 14(5)(e).
[160] Draft e-Evidence Regulation, Art. 2(3).
[161] Draft e-Evidence Regulation, Art. 2(4).
[162] European Data Protection Board (EDPB), 'Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)' (EDPB e-Evidence opinion), Adopted on 26 September 2018, pp. 9-10, available at: https://edpb.europa.eu/sites/default/files/files/file1/eevidence_opinion_final_en.pdf.
[163] EDPB e-Evidence opinion, p. 10.
[164] EDPB e-Evidence Opinion, p. 11. The EDPS adds a third distinct legal representative: that appointed under the future ePrivacy Regulation; EDPS e-Evidence Opinion, pp. 16-17.

4.1.1.2. EU Council – Delegation backed by sanctions

The first inroads into the Commission's direct cooperation model appeared in December 2018 with inclusion in the Council's general approach of a new Article 7a providing for notification of the competent authority of the putative enforcing state to take place simultaneously with the submission of orders to service providers.

However, such notification is limited to (i) European Production Orders only, concerning (ii) content data only, where (iii) the issuing authority has reasonable grounds to believe that the person whose data is sought is not residing on its own territory and (iv) entails submission to the enforcing authority of the EPOC only (the Certificate also received by service providers), rather than the Order itself – or both.[165] The automatic notification of the enforcing state as envisaged by the Council is further limited by the fact that it does not have a suspensive effect on the obligations of service providers,[166] meaning firstly that the 10-day window for production is unaltered and assessment by the notified authority must proceed swiftly.[167]

In its general approach, the Council thus largely maintains the Commission's positioning of service providers, but attempts to balance its own key priorities of national sovereignty and efficiency.[168] From a data protection perspective, as seen in Section 3.1. above, that role resembles much more the 'delegation' which is characteristic of data processors: an instruction is carried out with very little if any scope for decisional agency. Crucially, however, in this arrangement failure to perform the duty delegated would not result in (mere) data protection and/or contractual liability – but pecuniary sanctions under the e-Evidence Regulation, as determined by the 'enforcing authority'.[169]

4.1.1.3. The European Parliament – An express EIO for data

Draft amendments to the Commission proposals released by the European Parliament's Rapporteur in October 2019 insisted on a 'meaningful notification' of the rebaptised 'executing' – as opposed to 'enforcing' – authority. Notification, in the Rapporteur's view, can only be 'meaningful' if it includes the right to refuse to recognise data orders – and this in relation to all types of data – on the basis of grounds for non-recognition or non-execution set out in a new Article 10a.[170]

Those grounds are copied from the corresponding provisions in Article 11 EIO Directive, reflecting a general objective of refashioning the proposal into something of an 'express EIO for data', complete with a return to the familiar grounds for non-recognition or non-execution: optional for dual criminality; mandatory where a data order would be incompatible with a Member State's obligations in accordance with Article 6 TEU and the Charter.

---

[165] Council of the European Union, Document 10206/19 (Council e-Evidence general approach), 11 June 2019, Art. 7a. Notwithstanding agreement on the general approach, reservations were entered by no fewer than 19 Member States on several component parts of the reworked mechanism; *see* Council e-Evidence general approach, p. 34.

[166] Council e-Evidence general approach, Art. 7a(4).

[167] The notified authority's room for pushback is also minimal: it may inform the issuing authority of 'circumstances' related to immunities or privileges granted under its law, to ' rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media', or potential impact on fundamental interests such as national security and defence, but there is no power to object and the tenor of the new provision clearly puts the emphasis on production where at all possible.

[168] As in the priorities of the majority: a group of five Member States have made a reservation on this deletion, advocating, among others, the inclusion of a fundamental-rights clause in the provisions on conditions for issuing an EPOC(-PR), notification of the enforcing state and limitations on the use of data obtained; Council, Document 10206/19, p. 43.

[169] Draft e-Evidence Regulation, Arts, 13 and 14.

[170] European Parliament, Draft Report on the proposal for a regulation of the European Parliament and of the Council on European Production Orders for electronic evidence in criminal matters (Sippel Report), 24 October 2019, pp. 96-99.

Reverting to the more familiar EIO dynamic also has consequences in terms of data protection, and whilst (echoing the EDPB and EDPS) the Parliament proposed to narrow the personal scope of the Regulation to GDPR data controllers,[171] this is not the same as determining which legal regime is to apply to which part(s) of the cooperation chain: namely, when data travels from the service provider to the executing authority, and then onward to the issuing authority.

The EIO Directive itself until very recently provided, in its Article 20, that Member States were to ensure, when implementing that instrument, that personal data may only be processed in accordance with the 2008 Framework Decision and the principles of the Council of Europe's 'Convention 108'.[172] Even reading in the LED in place of the reference to its predecessor[173] was not sufficient to remedy a mismatch between the material scope of the LED (police and criminal justice) and other types of proceedings for which an EIO can be issued, which extend beyond criminal proceedings to include for instance punitive administrative proceedings.[174]

Although its July 2021 report on the implementation of the EIO Directive made no mention at all of data protection,[175] the Commission had already acknowledged this potential for confusion in a proposal to amend the EIO Directive[176] – a recommendation initially made in a Communication which had assessed the need, in the interests of consistency, for steps to align a wide range of Third Pillar instruments with the LED.[177] The chosen solution was to delete Article 20 EIO Directive, effective as of March 2022, via amending Directive 2022/228.[178] The result, that amending Directive states in a recital, is that the processing of personal data under the EIO Directive for the purposes set out in Article 82 TFEU *should* comply with the LED – 'where that latter Directive applies' – whereas processing of personal data under the EIO Directive in relation to formally non-criminal[179] proceedings mentioned in Articles 4(b), (c) and (d) EIO Directive, where the LED does not apply, the GDPR will.[180]

Member States had until 14 March 2023 to bring into force the laws, regulations and administrative provisions necessary to comply with this reform,[181] but it remains to be seen how far consistency and effective data protection (the twin goals of the reform)[182] can be improved by soft, qualified language included in the preamble. It will be important to monitor

[171] Sippel Report, Amendment 87, expressly binding the definition of 'service provider' to the role of data controller under the GDPR.

[172] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108), ETS No. 108, 28 January 1981. See further Section 4.2. below.

[173] As required by LED, Art. 59.

[174] *See,* EIO Directive, Art. 4(b)-(d).

[175] European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, [2021] COM(2021) 409 final, 20 July 2021.

[176] European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2014/41/EU, as regards its alignment with EU rules on the protection of personal data, [2021] COM(2021) 21 final, 20 January 2021, p. 4.

[177] *See,* European Commission, Communication to the Parliament and Council on the Way forward on aligning the former third pillar acquis with data protection rules, [2020] COM/2020/262 final, 24 June 2020, pp. 10-11. LED, Art. 62(6) called upon the Commission to review other legal acts adopted by the Union which regulate processing by competent authorities for LED purposes with a view to aligning those acts with the LED.

[178] Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data, [2022] OJ L 39/1-3, 21 February 2022, Art. 1.

[179] According to the seminal *Engel* jurisprudence from the European Court of Human Rights (*Engel and Others v. The Netherlands*, Appl. No. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, 8 June 1976; adopted by the CJEU in Case C-489/10, *Bonda*, [2012] ECLI:EU:C:2012:319, para. 37), an offence bearing the 'administrative' label in national law may nonetheless satisfy the ECtHR's (autonomous) interpretation of a criminal charge for the purposes of applying Art. 6 ECHR, depending on the nature of the (so-called 'punitive administrative') offence and the severity of the penalty. In its judgment in *Penalty Points*, the CJEU applied the *Engel* / *Bonda* jurisprudence in determining the applicability of Art. 10 GDPR ('Processing of personal data relating to *criminal convictions and offences*') to a system of public disclosure of penalty points deducted for road traffic offences; Case C-439/19, *Latvijas Republikas Saeima (Penalty Points)*, [2021] ECLI:EU:C:2021:504, paras 80-94.

[180] Directive 2022/228, Recital 2.

[181] Directive 2022/228, Art. 2(1).

[182] Directive 2022/228, Recital 2.

in future whether those Member States which had chosen to apply the weaker LED rules to administrative offences (including in purely domestic cases) now consider themselves obliged to revise national rules in order to bring EIOs issued (inherently, cross-border) in relation to punitive administrative proceedings under the higher standards of the GDPR.

Comparably, and to bring the discussion back to the e-Evidence reform, it will also be important to assess the risk of Member States construing the category of 'all criminal offences' so broadly as to cover administrative offences, thereby expanding the scope of the European Production Order.[183] Especially for data subjects and service providers, but also for investigators, legal clarity and consistency seem certain to prove a key challenge in this regard in years to come.

4.1.2. The gateway right: confidentiality and information to the data subject

In a delicate balancing act, Article 11 of the Commission's draft Regulation provides that the addressee of an EPOC or EPOC-PR must ensure the confidentiality of the order (and of the data produced or preserved) but shall only refrain from informing the person whose data is being sought (in compliance with Article 23 GDPR) where this is requested by the issuing authority. Where the service provider has not already informed the data subject that their data has been subject to an EPOC or EPOC-PR, it falls to the issuing authority to inform the target thereof once there is no longer a risk of obstructing the relevant criminal proceedings (in accordance with Article 13 LED). Once (if) apprised of the situation, the person whose data has been obtained via an EPO (whether a suspect or accused person or not; hence, whether in criminal or non-criminal proceedings) has the right to effective remedies under the EU data protection *acquis* and under national law before the court in the issuing state.[184]

The co-legislators' points of departure on Article 11 saw them at loggerheads: the Council's agreed position would ensure secrecy by default, with the issuing authority in virtually full control of whether to inform the target,[185] whilst the Parliament's Rapporteur has proposed to make notification by the addressee (rather than the issuing authority) the rule, with any exception requiring a court order.[186]

Meanwhile, some commentators suggested that '[t]he practical exercise of the right of data subjects to be informed could be enabled, for instance, through the involvement of trusted third parties (e.g. national data protection authorities)'.[187] Such a setup is vulnerable to the charge of raising more questions than it solves, not least in terms of workability and resources. Moreover, the main principled argument against involving DPAs in such a way – that to do so would radically alter their role in national criminal justice systems – stands to reason. At the same time, it is submitted, it is also surely worth reflecting on whether such a mechanism would be (much) less radical than the 'new dimension in mutual recognition'[188] entailing a relegation of the public hitherto-executing authority to a residual enforcement role, substituted in the base direct cooperation scenario with a private entity.

In any case, especially in light of the difficulties of preparing a criminal defence across borders in a likely unfamiliar jurisdiction, and a fortiori should the fundamental rights check on data orders by service providers be cursory or even removed (as proposed by the Council),[189]

[183] Under the Commission proposal, European Production Orders to produce subscriber data or access data may be issued for 'all criminal offences'. *See,* Draft e-Evidence Regulation, Art. 5(3).
[184] Draft e-Evidence Regulation, Art. 17. Importantly, immunities and privileges in respect of transactional or content data obtained by virtue of an EPO granted under the law of the Member State of the addressee (the service provider) are to apply in criminal proceedings in the issuing state.
[185] Council e-Evidence general approach, 38.
[186] Sippel Report, pp. 99-101.
[187] S. Carrera and M. Stefan, 'Access to Electronic Data for Criminal Investigations Purposes in the EU' (2020) 1 *Liberty and Security in Europe* 66.
[188] COM e-Evidence IA, p. 37.
[189] As discussed in Section 4.1.1.2.

notification of data subjects functions as a gateway right in order for further protections or defence rights to be invoked.[190] As such, it was certain that once the outcome of the lengthy trilogues eventually surfaced in the form of a compromise text, many data protection and criminal defence lawyers would make a beeline for the settlement arrived at in this specific respect.

In early 2023, just as this chapter was being finalised, that compromise text was released.[191] Although a full overview of its broader potential data protection ramifications is for future research efforts, the following sub-section offers a first glimpse of the freshly-agreed e-Evidence Regulation – beginning where this sub-section ends: with the notification of data subjects.

4.1.3. January 2023: agreement on e-Evidence

In terms of confidentiality and information to the data subject, the final version of Article 11 is most in keeping with the EU Council's late 2018 position, with a degree of compromise between co-legislators subtly visible in the structuring and contents of the provision.[192] Thus, as a rule the issuing authority shall inform the person whose data are being sought without undue delay;[193] there is no longer any mention of addressees or service providers informing data subjects.[194] However, an issuing authority may delay, restrict or omit informing the person whose data are being sought, to the extent that, and for as long as the conditions in Article 13(3) LED are met. Reasons for doing so must be indicated in the case file, and a short justification must be added in the Certificate.[195]

The settlement reached on notification of the data subject sits within an overall cooperation mechanism which blends elements from each of the co-legislators' visions. In terms of the 'directness' of that cooperation, Article 7a plays a crucial role. Reflecting the European Parliament's priorities, that provision establishes a system of notification with suspensive effect (except in emergency cases) of the competent authority of the 'enforcing state'.[196] However, its weight is subject to a double limitation. On the one hand, reflecting the Commission's initial wish to streamline access to less sensitive data categories, it only applies to content data and traffic data 'except when the latter is requested for the sole purpose of identifying the user'. On the other hand, reflecting the Council's stance, notification does not kick in at all – even to those more sensitive data categories – 'if, at the time of issuing the Order, there are reasonable grounds to believe that (a) the offence has been committed, is being committed or is likely to be committed in the issuing State; and (b) the person whose data are sought resides in the issuing State'.[197] Given the subjective nature of this pivot between indirect and direct cooperation, to be operated by issuing authorities, in future it will be essential that the transparency standards in the e-Evidence Regulation are upheld: in

[190] Carrera and Stefan, 'Access to Electronic Data', 53 – 57.

[191] Press release, 'Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence', Council of the European Union, 25 January 2023, available at: https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/.

[192] Council of the European Union, Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (e-Evidence final compromise text), [2023] 2018/0108(COD), 20 January 2023, p. 81.

[193] e-Evidence final compromise text, Art. 11(1). *See also,* Recital 43.

[194] Those entities are bound to ensure the *confidentiality, secrecy and integrity* of the EPOC or the EPOC-PR and of the data produced or preserved. *See,* e-Evidence final compromise text, Art. 11(3), emphasis added.

[195] e-Evidence final compromise text, Art. 11(2).

[196] e-Evidence final compromise text, Art. 7a(4). Accordingly, grounds for refusal for European Production Orders (immunites and privileges, freedom of the press and freedom of expression, manifest breach of 'a relevant fundamental right', ne bis in idem and double criminality) are set out in Art. 10a.

[197] e-Evidence final compromise text, Art. 7a(2).

particular, overall numbers of EPOCs issued[198] against the number of notifications sent to the 'enforcing state'.[199]

High levels of discretion for the issuing authority are also visible as regards the interface of the EU data protection *acquis* and the e-Evidence mechanism. The final compromise text specifies that European Production Orders 'shall be addressed to service providers, acting as data *controllers*, in accordance with [the GDPR]', or – exceptionally – to data *processors* where 'the controller cannot be identified despite reasonable efforts on the part of the issuing authority, or addressing the controller might be detrimental to the investigation'.[200] The bar is set at 'reasonable efforts', whilst a Recital explains:

> 'The delimitation between the roles of controller and processor with regard to a particular set of data requires not only specialised knowledge of the legal context, but it could also require interpretation of often very complex contractual frameworks providing in a specific case for allocation of different tasks and roles with regard to a particular set of data to various service providers. Where service providers process data on behalf of a natural person, it may be difficult in some cases to determine who the controller is, even where there is only one service provider involved'.[201]

The same provision also explains that a controller, even when identified, may not be a suitable addressee in the eyes of the issuing authority where that controller is a suspect or accused or convicted person in the case concerned 'or there are indications that the controller could be acting in the interest of the person subject to the investigation'.[202] Once more, the bar is set rather low, with the slightest risk of jeopardising an investigation warranting the directing of orders to a data processor.

Where processors receive orders, the rule is that they shall inform the controller – not of the fact of receiving an order, but 'about the production of the data'.[203] Whilst this wording is fuzzy (does it mean that the controller is apprised that data has already been produced, that data is about to be produced,[204] or merely that an order has been received?) it seems likely that the question is largely moot, given that the issuing authority may request on open grounds that the service provider refrain from informing the controller: 'for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings'.[205] In light of this discretion afforded to the issuing authority, it is regrettable to find no specific requirement in the final Regulation to record and report reasons for the choice to opt for direct cooperation with a data processor rather than a data controller, where the controller is identifiable, or indeed the reasonable efforts made to identify it before ordering data from a processor.

Lastly, it is worth underlining that whilst the final e-Evidence Regulation does engage with the data protection status (controller or processor) of addressees of a European Production Order and regulate interactions between those parties as well as the data subject, it makes no mention of the data protection regime(s) which may be applicable to the *transfer* of data to the relevant authorities.[206] It thus leaves unaffected the analysis made heretofore in this chapter, particularly in Sections 2 and 3.

---

[198] e-Evidence final compromise text, Art. 19(2)(a).
[199] e-Evidence final compromise text, Art. 19(2)(ba).
[200] e-Evidence final compromise text, Art. 5(6), emphasis added.
[201] e-Evidence final compromise text, Recital 34.
[202] e-Evidence final compromise text, Recital 34.
[203] e-Evidence final compromise text, Art. 5(6a).
[204] Compare the wording of the notification to be made in principle to the data subject, ie the person 'whose data *are being sought*'. *See,* e-Evidence final compromise text, Art. 11(1), emphasis added.
[205] Similarly to the mechanism for notification of the data subject, 'the issuing authority shall indicate in the case file the reasons for the delay. A short justification shall also be added in the Certificate' to be sent to data processors to explain why they must not inform the controller'. *See,* e-Evidence final compromise text, Art. 5(6a).
[206] *See e.g.,* e-Evidence final compromise text, Arts. 9(1a)-(1b).

4.2. The Second Additional Protocol to the Budapest Convention[207]

4.2.1. Direct cooperation under the Protocol, signature and ratification

As the e-Evidence reform inched its way toward finalisation throughout 2022, the EU was also preparing its reception of the Council of Europe's kindred spirit: the 2nd Protocol. In April 2022, the EU Council adopted a decision authorising Member States to sign the 2nd Protocol.[208] Signature and subsequently ratification would constitute the next milestones on the long path taken by the reform through the Cybercrime Convention Committee (T-CY) drafting process, which began in September 2017, before in June 2019 the Commission received a mandate from the Member States to begin negotiating the protocol directly with the Council of Europe.[209]

In the final agreed mechanism, direct cooperation consists of requests for domain name registration information (Article 6) and disclosure of subscriber information (Article 7).[210] For the former, there is no scope for Parties to enter reservations. For the latter, in contrast, a host of options exists. Parties may:

- Reserve the right not to apply Article 7 (Article 7.9.a.);
- Reserve the right not to apply Article 7 to 'certain types of access numbers' (Article 7.9.b);
- Make (upon signature or ratification) the following declaration: "The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision" (Article 7.2.b.);
- Notify (upon signature or ratification or at any other time) the Secretary General of the Council of Europe that, when an order for subscriber information is issued to a service provider in its territory, it requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation of proceeding (Article 7.5.a.) to a single designated authority.[211]

Whilst the overlap in core tensions with the EU e-Evidence reform addressed in some detail above is self-evident, it is important to highlight fundamental differences between the EU and Council of Europe initiatives – both related to the matter of whether and to what extent the latter are to be taken as legally binding.

First, at the 'lower' level of direct public-private cooperation in practice, unlike under the e-Evidence Regulation requests for direct cooperation under the 2nd Protocol would not necessarily be binding: in relation to both domain name registration information and subscriber information, '[t]he form of implementation depends on Parties' respective legal and policy considerations'.[212] In individual instances of cooperation, therefore, it will have to be

[207] *See also,* in this volume, A. Aguinaldo and P. De Hert.

[208] Council Decision (EU) 2022/722 of 5 April 2022 authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Council 2nd Protocol signature decision), [2022] OJ L 134, 11 May 2022, pp. 15-20.

[209] Press release, 'Security Union: Commission receives mandate to start negotiating international rules for obtaining electronic evidence', European Commission, 6 June 2019, available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2891. *See,* P. De Hert and A. Aguinaldo, 'A leading role for the EU in drafting criminal law powers? Use of the Council of Europe for policy laundering' (2019) 10 *New Journal of European Criminal Law,* 2, 99-106.

[210] Pursuant to Art. 5(7), the direct cooperation provisions in the 2nd Protocol do not restrict cooperation between Parties, or between Parties and service providers or other entities, through other applicable agreements, arrangements, practices, or domestic law. On this level, therefore, the EU e-Evidence reform is unaffected.

[211] *See,* Art. 7.5.b-f for further details of options and procedures on notification.

[212] *See,* Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Explanatory Report to 2nd Protocol), ETS No.

ascertained whether cooperation across the territorial borders of Parties is voluntary or mandatory, depending on the domestic arrangements of the Party hosting the headquarters or representative of the service provider.[213]

Second, at the 'higher' level, in the international setting differences in approach are routinely left in agreed texts in the form of explicit reservations or declarations – rather than being traded off or nuanced into a single compromise text, as is generally necessary for EU legislation.

In its twin proposals for Council Decisions respectively on the signature and ratification of the 2nd Protocol, the Commission had envisaged instructing Member States not to avail themselves of the two reservations listed above, but to ensure that they do make the declaration and notification listed subsequently, 'to ensure compatibility with the Commission's e-Evidence legislative proposals, including as the draft legislation evolves in the discussions with the co-legislators'.[214] By the time the final 'signature' decision was adopted, the EU Council had amended one of those two instructions: whereas Art.7.9.a. (a general opt-out from direct disclosure of subscriber information) remained on 'refrain', in respect of Article 7.9.b Member States were instructed that they 'may make such a reservation, but only in relation to access numbers other than those necessary for the sole purpose of identifying the user'.[215]

That instruction was one of two main reasons why the European Parliament's Rapporteur had proposed to reject the draft Council 'ratification' decision, for fear of different protection standards emerging inside the EU.[216] After agreement on the parallel EU e-Evidence reform had been reached, in January 2023 the European Parliament's LIBE Committee rejected the Rapporteur's draft resolution, thus paving the way for the adoption of the Council decision and ratification of the 2nd Protocol by the Member States on the proposed terms.[217] The final opt-out mirrors dovetails with the final text of the e-Evidence Regulation, which explicitly assimilates traffic data that is 'requested for the sole purpose of identifying the user' to the less sensitive category of subscriber data.[218]

4.2.2. To be continued: future impact on EU data protection standards

The European Parliament Rapporteur's more specific concerns had been voiced against the backdrop of the weaker data protection standards currently applicable to certain (non-EU and

224, 12 May 2022 para. 76 (domain name registration information) and para. 100 (disclosure of subscriber information).

[213] In this sense, aspects of the 2nd Protocol can be viewed as an evolution of the 'soft law' of T-CY Guidance Notes. *See in particular*, Council of Europe, T-CY Guidance Note #10. Production orders for subscriber information (Article 18 Budapest Convention), [2017] T-CY(2015)16, 1 March 2017, and for criticism P. De Hert, C. Parlar and J. Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law' (2018) 34 *Computer Law & Security Review,* 2, 327-336.

[214] European Commission, Proposal for a Council Decision authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence ('Draft 2AP Signature Decision'), [2021] COM(2021) 718 final, 25 November 2021, p. 9; European Commission, Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence ('Draft 2AP Ratification Decision'), [2021] COM/2021/719 final, 25 November 2021, p. 9.

[215] Council 2nd Protocol signature decision, Annex, '1. Reservations'.

[216] The other main reason concerned the suspensive effect of notifications to 'local' Parties under Art. 7(5a) 2nd Protocol. *See,* European Parliament, Explanatory Statement – Second Additional Protocol, 12 January 2023, available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2023/01-12/Explanatorystatement-SecondAdditionalProtocol_EN.pdf.

[217] Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (Council 2nd Protocol ratification decision), [2023] OJ L 63, 28 February 2023, pp. 48-53.

[218] *See,* e-Evidence final compromise text, Recital 22a.

non-Council of Europe) Parties to the 2nd Protocol. At the same time, the protocol itself represents a variegated instrument of data protection harmonisation. Although it goes beyond the purposes of this chapter to attempt to gauge the likely impact of the 2nd Protocol (of which direct cooperation is only one aspect) on EU data subjects, a few remarks on the data protection-specific aspects of the reform may be instructive.

Article 14 is the relevant dedicated provision in the 2nd Protocol, setting out a suite of data protection principles and safeguards which correspond to those in the GDPR and the LED: purpose and use, quality and integrity, sensitive data, retention periods, automated decisions, data security and security incidents, maintaining records, onward sharing within a party, onward transfer to another State or international organisation, transparency and notice, access and rectification, judicial and non-judicial remedies, and oversight.[219]

Here are certainly some notable iterations of the cornerstones of data protection law: for instance, Parties shall not further process personal data for a purpose which is incompatible with the initial '*specific* criminal investigations or proceedings',[220] a framework for dialogue between Parties is in place aiming to accommodate the requirements of Parties whose domestic legal framework requires 'personal notice' to the individual whose data have been collected (as opposed to the publication of 'general notices'),[221] and a Party may suspend the transfer of personal data under the 2nd Protocol if it has substantial evidence that the other Party is in systematic or material breach of the terms Article 14 or that a material breach is imminent.[222]

The latter safety net has been included, the Explanatory Report notes, since '[t]he drafters considered that the safeguards of this article and their effective implementation are essential […]'.[223] By the same token, however, that aim is liable to be undermined by the limited scope of application of Article 14 itself. On the one hand, its contents can only apply to data received under the 2nd Protocol.[224] On the other, it is disapplied in favour of 'comprehensive' mutually-binding international agreements on the same matters or if no such agreement is in place (so that they 'retain flexibility in determining the data protection safeguards that apply to transfers between them under the Protocol')[225] Parties may mutually determine that the transfer of data under the 2nd Protocol may take place on the basis of other (not necessarily comprehensive, not necessarily binding) agreements or arrangements.[226]

For many Parties, the relevant agreement is Convention 108 (and '108+' where appropriate).[227] Lack of space precludes a worthy analysis here of the 'comprehensiveness' of the modernised Convention 108 – both in terms of content and coverage – in the field of cross-border criminal investigations and proceedings, and of emerging direct cooperation powers in particular.

What remains to be specified, to close, is that the 2nd Protocol alone will have no effect on the application of the 'Umbrella Agreement'[228] between the United States and the European

[219] 2nd Protocol, Arts. 14.2 – 14.14.
[220] Emphasis added; 2nd Protocol, Art. 14.2.a. in conjunction with Arts. 2.1.a. and 2.1.b.
[221] 2nd Protocol, Art. 14.11.c.
[222] 2nd Protocol, Art. 14.15.
[223] Explanatory Report to 2nd Protocol, para. 282.
[224] 2nd Protocol, Article 14.1.a. Parties remain free to apply higher standards to processing by their own authorities under Art. 14.1.e.
[225] Explanatory Report to 2nd Protocol, para. 223.
[226] 2nd Protocol, Arts 14.1.b.-c.
[227] As mentioned in the Explanatory Report to 2nd Protocol, para. 222. *See,* Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), ETS No. 223, 10 October 2018. At the time of writing, 20 Members and non-Members of the Council of Europe (of which 13 are EU Member States) had both signed and ratified/acceded to the Protocol. Ireland has signed the Protocol, but not yet ratified it.
[228] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (Umbrella Agreement), [2016] OJ L 336, 10 December 2016.

Union – as is confirmed in the Explanatory Report.[229] From the opening in mid-2019 of negotiations in view of an EU-US agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters, it has been common ground on the European side that the Umbrella Agreement clearly needs to be complemented with 'additional safeguards that take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities and transfers from competent authorities directly to service providers'.[230] Once more, the ball is back in the Commission's court.

5. Conclusion

This chapter set out to shed light on the relationship between EU data protection law and public-private 'direct cooperation' – in its multiple configurations, whether mandatory or voluntary – on digital evidence in criminal investigations.

It built on well-established literature focusing on the transatlantic e-Evidence paradigm, as typified by the *Yahoo!* and '*Microsoft Ireland'* cases and the reforms launched in their wake, seeking to form a more complete view of relevant law and practice within Europe so that the data protection ramifications of the ongoing drive toward formalised and intensified mechanisms for direct cooperation may be better grasped. The scope of the analysis thus zoomed both further in and further out than the EU's e-Evidence package and the US CLOUD Act. It zoomed in, for instance, by examining the legal regimes that apply where direct cooperation is of an entirely domestic nature but nonetheless triggers EU data protection law, and it zoomed out, for example, by broaching the future role of EU data protection standards in the Council of Europe's own new direct cooperation facility, that of the Second Additional Protocol to the Budapest Convention.

The chapter detailed how the kinds of private-to-public data transfers for criminal investigations that used to fall (pre-GDPR) into the gap between separate regimes conceived respectively for private and public data processing are now subject to a degree of regulatory overlap. The *lex generalis* GDPR potentially applies whenever the *lex specialis* LED does not, and in some cases both instruments may apply. Given the discrepancies in levels of protection afforded by the two regimes, the question of which one is to apply to what stage(s) of any instance of public-private direct cooperation demands clarification. In taking up that gauntlet, the chapter distinguished between three scenarios of formal direct cooperation (along with one further scenario, that of informal or voluntary cooperation) and viewed those scenarios through the prism of data controllership.

Whilst the black-letter analysis revealed a hazy normative picture, with information on national implementations of the LED still fragmented, a conceptual-theoretical perspective identified several questions around the internal consistency of EU data protection law that remain on the table – despite the important contributions of the CJEU in recent years. Ultimately, the chapter argued that the bifurcated edifice of the EU data protection *acquis* continues to be fundamentally challenged by data processing that shifts between 'public' and 'private' realms, whether in isolated instances or in the course of more stable partnership-like arrangements, inherently engaging both GDPR and LED.

Most evidently, the purpose limitation principle risks being effectively emptied should data handled by private service providers slip from the ambit of the GDPR to the prosecutor, judge, police or other competent authority, operating (for core purposes) under the LED. Even if the position is assumed that investigative needs trump purpose limitation, this chapter has maintained that the effective fulfilment of data subject rights (and of independent supervision)

[229] Explanatory Report to 2nd Protocol, para. 222.
[230] Draft 2AP Signature Decision, 7-8; Draft 2AP Ratification Decision, 7-8.

can only be hampered by such levels of indeterminacy as regards the applicable legal regime(s).

The European Commission's 2018 e-Evidence package did not engage with these questions, opting to refer to the EU data protection *acquis* in general. Had it explicitly engaged with the notions of data controller and data processor, this chapter posited, the criteria for joint controllership over the transfer may well have been met by the proposed scheme. The final text, released in January 2023, delivers a production order that is most aligned with the Council's enforcement-oriented priorities, but containing elements of the Parliament's mutual recognition-based vision. Although the question of the law that might apply to the transfer of digital evidence thus goes unanswered (is the e-Evidence Regulation to be considered the *passerelle* for data travelling from GDPR to LED?), data protection has not been lost in the wash: the new mechanism comes with a much-revised regime for the notification of data subjects. A first look suggested that both the wording of that regime and the transparency requirements related thereto could have been more finely tuned, so that in future it will be possible to precisely gauge the impact of the new reform on the effective fulfilment of data protection standards within the EU.