Cambridge Law Journal, page 1 of 29. © The Author(s), 2025. Published by Cambridge University Press on behalf of The Faculty of Law, University of Cambridge
doi:10.1017/S0008197325100962

EU DATA NULLIFICATION: CONFUSION AND THE RULE OF LAW

PETER CHARLETON* AND VICTORIA O'CONNOR**

ABSTRACT. *Effective justice seeks for the truth and consequently must be founded on an analysis of all relevant evidence. Only where a manifestly greater societal interest intrudes, can there be a privilege against the production of testimony. For the Court of Justice of the EU, however, an activist interpretation of Article 8 of the EU Charter, promoting security of data, has become an elevated privacy right which justifies nullifying crucial information, thus shielding criminals, undermining civil trials and obstructing searches for missing persons. No convincingly apodictic conclusion emerges from the several judgments of the court, while the exceptions identified undermine, rather than support, any articulated core principle.*

KEYWORDS: judicial activism, metadata, nullifying proof, victims' rights.

I. INTRODUCTION: FORMING LAW, COURTS AND LEGISLATURES

Exclusionary rules of evidence can be inimical to the truth-seeking function of the administration of justice. In parallel with civil law systems, common law uses compulsion to adduce all relevant evidence before the tribunal of fact. Axiomatic to satisfying the demands of the equitable maxim "the law is entitled to the evidence of every man" is that the system is presented with all material evidence except for witnesses and data that are privileged by law.[1] A rule of law to exclude relevant evidence is required and, in turn, must be supported by reasoning that, by its common sense, convinces society that some greater good justifies its loss. Rules of exclusion, thus, for any robust legal system, are an exercise in proportionality. In the EU supranational legal order, however, the jurisprudential evolution of the right to the protection of privacy and personal data as applied to the retention and access to telecommunications data for law enforcement has been ensnared by the protection of excessively abstract rights to the diminution of concrete fundamental rights protection.[2]

*Peter Charleton, writing in a personal capacity, is a judge of the Supreme Court of Ireland and is adjunct professor of criminal law and criminology in the University of Galway.
**Victoria O'Connor, at time of writing, was a researcher attached to that court. Both are graduates of Trinity College, Dublin. Address for Correspondence: The Four Courts, Dublin 7, Ireland. Emails: petercharleton@courts.ie; oconnovi@tcd.ie.

[1] *The People (D.P.P.) v J.T.* (1988) 3 Frewen 141 (I.E.C.C.A.).
[2] See S. O'Leary, "Balancing Rights in the Digital Age" 59 (2018) Irish Jurist 59.

No convincing balancing principle is found in the several pronouncements of the Court of Justice of the EU ("CJEU") whereby the gathering of inert data as to telephone communications is described as "interception" or "surveillance of communications" and whereby, in consequence of the elevation of privacy in metadata,[3] courts throughout the EU are shorn of what has become a fundamental tool in the search for truth. Evidence is simply made to disappear and that is not always justifiable, even as a bulwark against executive intrusion. Fundamental to the CJEU's approach is to undermine surveillance. The defining feature of bulk surveillance is that it allows public authorities to have access for specified purposes to large quantities of data, though "a significant portion of the retained data pertains to identifiers that are not targets at the time of collection".[4]

Purpose, context and culture are, however, central to the understanding of surveillance.[5] The exclusionary fate of most metadata evidence is a single cog, with the most profound consequences, in the wider machinery of social ordering that defines the surveillant society of today.[6] The Internet, by its nature, "smudges the distinctions between monitoring and tracking activities of security agencies, police and corporate marketers and advertisers and the surveillance initiatives of everyday life".[7] Academics warn of the implications of "surveillance capitalism … [defined as] the unilateral claiming of private human experience as free raw material for translation into behavioral data" on democracy and agency.[8] While these ideas are concerning, their expression in the form of sweeping exclusionary rules of evidence, in nullifying metadata as a tool of litigation, is in error. Experience teaches that justice wears different faces. Hence, there may be differing solutions to the promotion of data privacy; but nullifying an entire category of cogent evidence from judicial scrutiny requires strong reasoning.

[3] Metadata or "non-content data" refers to data about who communicated, when, for how long and where. The CJEU refers to this as "traffic and location data", including (1) Subscriber: identifying the subscriber, (2) Traffic: routing, duration, time, volume protocol, location and network details, and (3) Location: coordinates, direction, accuracy and network cell.

[4] US National Research Council, *Bulk Collection of Signals Intelligence: Technical Options* (Washington, DC 2015). Note, *Collins Dictionary* defines "surveillance" as "the careful watching of someone, especially by an organisation such as the police or army".

[5] D. Lyon, "Surveillance" (2022) 11 Internet Policy Review 1.

[6] David Anderson Q.C., writing as the Independent Review of Terrorism Legislation, observed in 2016 that "whether a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to mass surveillance. Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data is not given on an indiscriminate or unjustified basis"; see D. Anderson Q.C., *Report of the Bulk Powers Review*, Cm 9326 (London 2016), at [1.9].

[7] D. Lyon, "Surveillance Capitalism, Surveillance Culture and Data Politics" in D. Bigo, E. Isin and E. Ruppert (eds.), *Data Politics: Worlds, Subjects, Rights* (London 2019), 65.

[8] J. Laidler, "High Tech Is Watching You", available at https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ (last accessed 17 June 2025); see also S. Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (London 2019).

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

Metadata gathering for commercial purposes is not mass surveillance. It is the random collation of otherwise incomprehensible observations as to the use of mobile and fixed telephony and the routes travelled. That is no more than what a witness might observe who happens upon a criminal or a civil wrong. While, by definition, wide powers of surveillance raise legitimate privacy concerns, because of potential access of the state to wide data sets and the resulting risk of abuse, in themselves, these factors are not a reason for generally presuming that every item of retained data should be put beyond the use of the justice system. But, in a series of cases, the CJEU has proclaimed the need to protect any personal or professional use of data. That court has taken Article 8 of the Charter of Fundamental Rights of the EU ("EU Charter"), merely guaranteeing within the EU "the right to the protection of personal data concerning him or her", as a justification for occluding vital information from the justice system.

The importance of these cases lies in their confirmation of the CJEU's expansive interpretation of its own jurisdiction, arguably bordering *Kompetenz-Kompetenz*, and in its willingness to exercise activist judicial review over EU legislation. Given the ubiquity of communications data, the approach has far-reaching consequences for evidence in the EU legal order; including the exoneration of suspects, crimes in action (kidnap for ransom, blackmail), trafficking (people, narcotics or weapons), crimes of violence, including assault, harassment and murder (when communications data can corroborate new information, often some-time after the event).[9] In the emphatic fashioning of a new principle of data nullification, furthermore, the CJEU's grafting of exceptions emerges as more likely to undermine any internal logic of whatever reasoning originated the doctrine, rather than highlighting the soundness of its general justification.

Where courts fashion law,[10] the fabric of judicial pronouncement invariably purports merely to be development; the application of existing principle to novel challenges.[11] Lawyers raised on common law understand how necessity may parent judicial invention in pursuit of justice.[12] Yet, even there, first, the warp of the new fabric will be closely scrutinised for conformity with the weft of acceptable precedent and, second, for judicial activism to prevail, the internal logic must be so especially sound as to support, perhaps excuse, the exercise of creativity in law.

[9] D. Anderson Q.C., *A Question of Trust: Report of the Investigatory Powers Review* (London 2015), at [9.25].

[10] In the US, *Miranda v Arizona* 384 U.S. 436 (1966) established rights for those arrested and interrogated by the police, while *Mapp v Ohio* 367 U.S. 643 (1961) applied the exclusionary rule to unlawful searches and seizures to states as well as the federal government.

[11] E.g. *The People (D.P.P.) v McNamara* [2020] IESC 34, [2021] 1 I.R. 472, at [32] (Charleton J.), in which the Irish Supreme Court radically restated the defence of provocation. Changes can also be problematic and critiqued for that very willingness to develop the law; see A. Chronopoulos, *Judicially Crafted Property Rights in Valuable Intangibles: An Analysis of the INS Doctrine* (London 2024).

[12] O. Wendell Holmes Jr., *The Common Law* (London 1911), ch. 8.

A. Metadata Collection: Overview

Since the nineteenth century, governments have generally required access to user communications; justified by the fight against crime and national security.[13] With the invention of the mobile phone, proof that a call was made no longer established location or that a particular occupant may have made it. As mobile devices became gracile, the sophistication of computer chips enabled storage of numbers and Internet access through computer-enabled devices.[14] All of these developments were commercial. Billing was justified by proof of use. Hence, analogue devices were used in telephone exchanges to record the length of calls and routing in fixed telephony. Issues of location did not then exist. Itemised phone bills showed this data. With mobile, a new element was added; that of shifting location. Second by second, when a device is in use, its location may be digitally discernible. For billing purposes, the time, duration, the mast from which a caller is routed and to which the signal connects the receiver supports a charge. Critically, this also provides potentially important information in searches for missing persons and for criminal and civil litigation. Where a user consents, as in the use of online direction-finding services, mobiles can be accessed to show traffic build-up without the use of the device to make a call or message. With commercially held traffic data, the original routing mast and the receiving mast do not change even though both caller and receiver are travelling. If either move out of range, the signal is degraded or lost. The mast used to locate the device is usually, but not always,[15] that which is closest to the caller and to the receiver with devices connecting to one of the thousands of individual geographic cells, generally encompassing a 40-kilometre radius.[16]

From analogue landline invoicing to continuous digital connection with an active device, service providers first gathered data for billing but then began using location, travel, connectivity and consumer trends as a saleable commodity. The first EU law intervention in telecommunications, within the competence of the 1957 Treaty of Rome, Articles 86 and 95, aimed at creating a genuine internal market, geared towards the abolition of exclusive commercial rights. The liberalisation and harmonisation process of the telecommunication's regulatory environment[17] generated a new interest, namely data processing. By the 1970s, to mitigate US market domination,

[13] D. Ventre and P. Guillot, *Electronic Communication Technology Interception Technologies and Issues of Power* (Newark, NJ 2023), 9.
[14] E.G. Hall, *The Electronic Age: Telecommunications in Ireland* (Dublin 1993).
[15] A call made from a vehicle when the closest mast is occluded, for instance by a metal lorry, may route through a more distant mast.
[16] Cell size depends on terrain; masts are usually built 200–500 metres apart in towns and 2–5 kilometres apart in rural areas but may be closer.
[17] See J. Scherer (ed.), *Telecommunications Law in Europe: Law and Regulation of Electronic Communications in Europe*, 6th ed. (Haywards Heath 2013).

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

the Commission published a "Community Policy on Data Processing". In 1993, the Maastricht Treaty introduced explicit telecommunications policy goals.[18]

B. Use of Words: Mass Surveillance

In themselves, words may be chosen to carry an emotional charge. Multiple references in the decisions of the Court of Justice to "mass surveillance" and the "ability to examine the past"[19] transport the inherently commercial and incomprehensibly stored nature of billing information into the realm of George Orwell's *Nineteen Eighty-Four*.[20] That is not so. As contact is made between telephonic devices, the service providers collect data for billing purposes. This activity could be referenced as surveillance where consumers are monitored as to their presence in particular locations in order to track their movement. No such intention is present in either the process or, more especially, in the way the data is harvested and stored. On the contrary, the Commission Study on Data Retention posits that identification and location data have limited business value and are retained for much shorter periods of time than other types of data.[21] What is collected, however, is data in potential, for proof, months after a communication to support a billable service. Across the EU, the average legal threshold for invoice contestation is three months.[22] Service providers may also retain data to comply with legal obligations such as tax and audit regulations. That data, unlike personal surveillance, is incomprehensible unless subject to specialised accessing and processing. No one within the EU is under surveillance because a commercial entity keeps information to support charges.[23]

Since mobile use is near universal, billing data is vast.[24] Keeping it on servers is problematic and transfer onto magnetic tape can be the preferred solution. These are neither accessible, comprehensible in themselves nor of any interest to the service providers beyond proof of accurate charging. Where legislation provides that this inert data should be kept beyond the period natural to a commercial dispute,[25] it is inert

[18] Now found in Consolidated Treaty on the Functioning of the European Union (OJ 2012 C 326 p. 47), arts. 170–172 (hereafter, "TFEU"), requiring "the Union [to] contribute to the establishment and development of trans-European networks in the areas of transport, telecommunications and energy infrastructures".

[19] *Tele2 Sverige A.B. v Post-och Telestyrelsen and others*, C-203/15 and C-698/15, [2017] Q.B. 771, at [180] (Saugmandsgaard Øe A.G.) (E.Ct.H.R.).

[20] G. Orwell, *Nineteen Eighty-Four* (London 1949).

[21] European Commission, *Final Report: Study on the Retention of Electronic Communications Non-Content Data for Law Enforcement Purposes* (Luxembourg 2020), 16.

[22] Ibid.

[23] In Member States, real-time interception and recording of communications require judicial authorisation by warrant on proof of reasonable suspicion of criminal culpability.

[24] Hall, *Electronic Age*.

[25] Here, the only limitation is that the relevant provision of legal limitation not be exceeded for what would ultimately be classified as a contract dispute.

and requires multiple processes to retrieve and to turn it into intelligible language. Only at the end of specialist processing may comprehensible information emerge; excluding content, (which is not recorded) and limited to number A calling number B at # time and for # seconds. The Europol, Eurojust and the European Judicial Network 2024 Report on Cross-border Access to Electronic Evidence in Criminal Investigations and Proceedings observes that it is often this type of data that constitutes the only investigative lead.[26]

II. EU Legislation: CJEU Activism

Article 2 of the Treaty on European Union ("TEU") founds the EU's legal order "on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities".[27] Crime infringes human rights, going so far as the removal of all rights through violent death. The Charter of Fundamental Rights of the EU ("The Charter"), while enshrining "the fundamental rights people enjoy in the EU" is cast as "a modern and comprehensive instrument protecting and promoting people's rights and freedoms in the light of changes in society, social progress and scientific and technological developments".[28] According to the Preamble, the instrument "reaffirms" fundamental rights, as these result from the "constitutional traditions and international obligations common to the Member States".[29]

Article 8 has been used as the justification by the Court of Justice for data nullification, whereby definite proof of human rights violations is hidden from Member States' justice systems. In full, it is qualified and merely provides:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

[26] Europol, Eurojust and European Judicial Network, "SIRIUS EU Electronic Evidence Situation Report 2024", available at https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (last accessed 4 December 2024).
[27] Consolidated Version of the Treaty on European Union (OJ 2008 C 326 p. 13), art. 2 (hereafter, "TEU").
[28] European Commission, "Why Do We Need the Charter?", available at https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-fundamental-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en#:~:text=The%20Charter%20enshrines%20the%20fundamental,and%20scientific%20and%20technological%20developments (last accessed 21 November 2024).
[29] Charter of Fundamental Rights of the EU (OJ 2012 C 326 p. 391), preamble (hereafter, "The Charter").

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

Limitations to the exercise of fundamental rights are governed by Article 52(1) of the Charter, which provides that "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms" and that "subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights or freedoms of others".[30]

A. Undermining Justice

No legal provision may validly be read in isolation. Article 47 provides that all "whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article". That requires "a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law".[31] Without the potential to access and analyse inert commercial metadata for strictly limited purposes in serious criminal investigations, much grave crime will remain undetected. Relevant evidence, by fiat of judicial activism, will be excluded from use as proof.[32] Investigators will be shorn of an indispensable tool for detecting violators. Justice should be an energetic search for the truth: and upon the truth alone is any fair verdict against an accused person or any response to human rights violations properly based.[33] Cutting out the truth, in the form of useful and convincing evidence, leads to the distortion of the legal process and its severance from good sense. But, have we really arrived at this situation; and if so, how?

B. Development

The evolution of primary and secondary law *acquis* on data protection and retention across the EU engages a complex history. Concisely, its development can be traced from a state-by-state approach to, in theory, the ultimate policy ambition of a harmonised model. While integration failures in this area loom large, the legal framework can be broadly understood as embracing (1) protection and (2) retention. These branch into subcategories regarding data harvesting for serious criminal investigations:

[30] Ibid., art. 52(1). Directive 2002/58/EC (OJ 2002 L 201 p. 37), art. 15(1) reflects a similar provision (hereafter, "ePrivacy Directive").
[31] The Charter, art. 47.
[32] Europol, Eurojust and European Judicial Network, "SIRIUS Report", 16.
[33] *Ó Grioföin v Éire* [2009] IEHC 188, [2009] 4 J.I.C. 2308, at [10]: "Is é an ceartas an aidhm atá le gach imeacht dlíthiúil. Is í an fhírinne an cuspóir atá ag gach cleachtas breithiúnach" (Charleton J.) (Justice is the aim of every legal proceeding. Truth is the target of all judicial practice).

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

(i) Data seizure: any electronic device according to the jurisprudence of the US,[34] Ireland,[35] the UK[36] and Canada[37] is subject to a specific justification in a search warrant application.
(ii) International data transfers: EU law requires a company operating in the EU that transfers personal data to a company in a third country to abide by specific requirements for data transfers under the General Data Protection Regulation ("GDPR").
(iii) Third-party discovery: this is the mechanism in civil cases whereby the right of a court to have access to all relevant evidence is engaged.[38] While civil law systems generally do not engage with discovery, there are mechanisms whereby a court can compel the production of what is relevant.
(iv) Data retention in the investigation of national security threats, crime and the recovery of missing persons.

Member States with civil law systems were early adopters of data protection laws,[39] while Member States with common law systems saw the incremental development of the tort of privacy. Internationally, harmonisation began with the Council of Europe's 1981 Convention 108.[40] In 1990, the European Commission adopted proposals for the protection of personal data.[41] The Commission considered that the diversity of national approaches to data retention threatened integration.[42] The aim of national laws in the field, the Commission suggested, was to "protect the fundamental rights of individuals, and in particular the right to privacy" and to further the aim of an internal market.[43] The original treaties of the European Communities are silent on data protection. The EU adopted its first comprehensive data protection instrument in 1995: Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data ("Data Protection Directive").[44]

[34] *Katz v United States* 289 U.S. 347 (1967).
[35] *The People (D.P.P.) v Patrick Quirke* [2023] IESC 5, [2023] 1 I.L.R.M. 225.
[36] *R. v C.B.* [2020] EWCA Crim 790, [2021] 1 W.L.R. 725.
[37] J.A. Fontana and D. Keeshan, *The Law of Search and Seizure in Canada*, 8th ed. (Markham, Ont. 2010), 1181.
[38] In England and Wales, the Civil Procedure Rules 1998, Part 31, and in Ireland, the Rules of the Superior Courts, SI 1986/15, order 31, rule 29 require non-parties to disclose relevant documents or data that may support civil litigation.
[39] E.g. the German state of Hesse adopted the first law on data protection in 1970, only applicable there.
[40] Council of Europe, "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" (ETS No. 108, adopted 28 January 1981).
[41] European Commission, "Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data" (OJ 1990 C 277 p.3).
[42] Ibid., rec. 5.
[43] Ibid., rec. 7.
[44] Directive 95/46/EC (OJ 1995 L 281 p.31). Data protection law was modernised in 2016 by the adoption of Commission Regulation (EU) 2016/679 (OJ 2016 L 119 p.1) (hereafter, "GDPR"). The General Data Protection Regulation also repealed the Data Protection Directive. Discussion of this Regulation is beyond the scope of this analysis.

Directive 97/66/EC ("Telecommunications Directive") was one of the earliest frameworks addressing data retention and privacy in e-communications.[45] It allowed for derogations from the obligations contained in the Directive where necessary for national security, defence, public security or law enforcement. It was replaced by the ePrivacy Directive. Most at issue has been the extent of derogations contained in Article 15 of the ePrivacy Directive which allows Member States to adopt legislative measures restricting the scope of the rights and obligations provided for in Articles 5, 6, 8(1), (2), (3), (4) and Article 9 of the Directive when necessary and proportionate to "safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".[46] Formerly, the trend was for the court to leave the assessment of Article 15 to Member States, but that has since changed, thus casting the court into the political arena.[47]

Following the terrorist attacks in New York, Washington, DC and Pennsylvania in September 2001, communication data was declared a useful criminal justice instrument.[48] After the terrorist attacks in Madrid in 2004 and London in 2005, the Council of Europe proposed the enhancement of EU security infrastructure.[49] An EU-wide data retention measure was passed in EU Directive 2006/24/EC ("the Data Retention Directive"), justified in the name of protecting the internal market.[50] The Directive provided for the retention of communication data for a period of between six and 24 months for the purpose of investigating, detecting and prosecuting serious crimes. Required retention included the data necessary to trace and identify the source of communication and its destination; to identify the data, time, duration and type of communication; to identify users' communication equipment; and to identify location.[51]

C. Case Law

The early contours of the CJEU's position on data retention thus reflect an enmeshment of factors, including fundamental rights protection, internal security and competence creep. Commentators largely fall into two

[45] Directive 97/66/EC (OJ 1997 L 24 p.1).
[46] ePrivacy Directive, art. 15.
[47] E. Kosta and I. Kamara (eds.), *Data Retention in Europe and Beyond* (Oxford 2025).
[48] S. Thierse and S. Badanjak, *Opposition in the EU Multi-Level Polity, Legal Mobilization Against the Data Retention Directive* (Cham 2021), 15.
[49] The council explicitly stated that "the priority should be given to the proposals under the retention of communication and traffic data and exchange of information on convictions with a view to adoption by June 2005"; see Council of the European Union, "Declaration on Combatting Terrorism", available at https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf (last accessed 29 July 2025).
[50] Directive 2006/24/EC (OJ 2006 L 105 p.54) (hereafter, "Data Retention Directive"). The legal basis for the Data Retention Directive was controversial from the start. The Irish government initiated the first challenge of the Directive before the CJEU on the basis that the Data Retention Directive was not appropriately adopted; see Judgment of 10 February 2009, *Ireland v European Parliament and Council of the European Union*, C-301/60, EU:C:2009:68.
[51] Data Retention Directive, art. 5.

camps: (1) privacy advocates who emphasise the growing volume of electronic communications and the extended techniques for their gathering and analysis in consequence of the digitalisation of our societies or (2) those, such as law enforcement authorities, who point to the decline in the proportion of electronic communication which they can access within a fragmented legal landscape.[52]

In the 2014 decision *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others*,[53] the CJEU invalidated the Data Retention Directive. The Court concluded that failings relating to both the retention and access regimes prevented it from attaining the necessary level of clarity and precision. This was classified as a "particularly serious" interference with fundamental rights "as the fact that the data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the person concerned that their private lives are the subject of constant surveillance"[54] – the right being, to use traditional terminology, that of privacy. But, as the body politic has developed an entirely separate and elevated right not to have one's data explored, scrutinised, revealed or used in the justice system, save in exceptional and defined circumstances, the intrusion of this notoriously vague concept could be predicted to flower strangely, as it has. The court held that the Directive:

- allowed Member States to introduce indiscriminate data retention regimes and did not limit the retention to data that is at least remotely linked to a serious crime;[55]
- did not establish objective criteria to restrict the access and use of data by national authorities, and in particular did not foresee any prior review by a court or an independent administrative body;[56]
- did not provide for substantive and procedural safeguards relating to the access and subsequent use of data by national authorities;[57]
- imposed fixed ranges of retention periods and did not allow national legislation to define them flexibly, according to the specific purposes of the retention;[58] and
- did not lay down rules concerning the security of the data retained by electronic communication providers, and in particular did not provide for the irreversible destruction of data and for their storing within the EU.[59]

[52] Anderson, *Question of Trust*, at [1.7].
[53] Judgment of 8 April 2014, *Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural Resources and Others*, C293/12, EU:C:2014:238 (hereafter, "*Digital Rights Ireland*").
[54] Ibid., at [37].
[55] Ibid., at [58]–[59].
[56] Ibid., at [60].
[57] Ibid., at [61]–[62].
[58] Ibid., [63]–[64].
[59] Ibid., at [66]–[68].

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

While the storage of data on an open-ended basis is potentially problematic, it does not follow that later use of metadata is unjustified. Following that pronouncement, challenges to national data retention regimes flared up throughout the EU with multiple references under the preliminary reference procedure of Article 267 of the Consolidated Treaty on the Functioning of the European Union ("TFEU"). Since 2016, the CJEU has repeatedly had to address issues exposed by their invalidation of the Data Retention Directive.

In *Tele2 Sverige v Watson and Others*,[60] the CJEU developed *Digital Rights Ireland* to invalidate national statutes supposedly implementing the Directive, justifying their decision on the fact that the national legislation was exercising the derogation provided by Article 15 of the ePrivacy Directive. The Court posited novel propositions. First, that only a system of "targeted data retention"[61] would conform to a combined reading of the ePrivacy Directive and the Charter. Second, that any national law providing for the retention and access to traffic and location data was made subject to a series of mandatory requirements:

> national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary.[62]

In the *dispositif*, the CJEU ruled that Article 15(1) of the ePrivacy Directive "read in the light of Articles 7, 8 and 11 and Article 52(1) of [the Charter]" precluded national legislation "which for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication".[63] Those same provisions precluded national legislators providing for access to the retained data "where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime [and] where access is not subject to prior review by a court or independent administrative authority".[64] At this point, using metadata to fight serious crime, potentially also to find missing persons, had not yet been nullified. Concepts of what was targeted, meaning geographic- or

[60] Judgment of 21 December 2016, *Tele2 Sverige A.B. v Post-och Telestyrelsen and others*, C-203/15 and C-698/15, EU:C:2016:970 (hereafter, "*Tele2*").
[61] Ibid., at [108].
[62] Ibid., at [109].
[63] Ibid., at [62].
[64] Ibid., at [114].

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

suspect-focused and of distinctions between state security and protecting citizens from crime had, however, now branched off from the original concept of what was a permissible interaction with privacy.

But exempting serious crime from a targeted retention regime was quickly lopped off. In *La Quadrature du Net v Premier Ministre and Others*,[65] the CJEU declared that the importance of the objective of safeguarding national security went beyond that of the other objectives in Article 15(1). General retention for state security was possible, but, for even the most serious crimes there had to be a level of prediction. The CJEU required this to be based on a rational suspicion that in a geographical area, criminal activity justified the retention of data or that individuals could be monitored because they were already assessed as likely to be involved in serious crime. This was not evidence-based. It is pure imagination. Crime is international and if crime could be predicted to the point of total accuracy, criminal activity would wither away. The threat to national security, further, must be shown to be "genuine and present or foreseeable".[66] Foreseeability, as a concept, creates interpretive difficulties since a future threat to national security could be foreseeable, but not necessarily imminent.[67] In the exceptional circumstances where national authorities can access such data, even that retention could not be systemic in nature and would have had to be subject to review either by a court or an independent administrative body.[68]

Hence, a state security threat can justify general retention with later access subject to the safeguard of judicial scrutiny. Outside of state security, crime detection requires foresight at an impossible level. Even the positive obligations that might arise under Articles 3, 4 and 7 of the Charter, establishing rules to facilitate effective action to combat criminal offences, could not have the effect of justifying interference with traffic and location data of practically the entire population "without there being a link, at least an indirect one, between the data of the persons concerned and the objective pursued".[69] The common law concept of reasonable suspicion, a rational safeguard, here metamorphosed into reasonable prediction based on current behaviour: otherwise, for the CJEU, grave crimes did not justify the retrieval of evidence in the form of metadata.

Persons identified as posing a serious criminal threat could be targeted once those persons had been detected beforehand on the basis of

[65] Judgment of 6 October 2020, *La Quadrature du Net and Others v Premier Ministre and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791 (hereafter, "*La Quadrature du Net*").
[66] Ibid., at [168].
[67] V. Mitsilegas et al., "Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks" (2023) European Law Journal 176, 191.
[68] Judgment of 6 October 2020, *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, at [139].
[69] Ibid., at [145].

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

"objective evidence",[70] or data could be retained on the basis of a geographic criterion, targeting areas of high crime or places particularly vulnerable to the Commission of serious crimes.[71] The CJEU also promoted expedited retention. In non-terrorist crime, data could be retained and later analysed, but only if based on a prediction. Reasonably suspecting someone of a crime that has happened requires a logical exercise in justifying a search or an arrest, but reasonable prediction as to what may occur in the future engages speculation. In line with its previous decisions, the CJEU emphasised the primacy of EU law over national legislation and to the designation in the Treaty on European Union of national security as the "sole responsibility of each member state".[72] But, if law enforcement authorities were legitimately investigating a terrorist incident or threat, what if evidence as to murder was uncovered?

If there was any doubt, the decision in *Bundesrepublik Deutschland v SpaceNet A.G. and Telekom Deutschland GmbH*[73] confirmed that a legislative measure laying down a retention of traffic and location data (10 weeks and four weeks, respectively) and rules intended to ensure the effective protection of the retained data against the risks of abuse and against unlawful access to those data sets could not be regarded as constituting a targeted retention scheme. As to the definition of "serious crime" the CJEU clarified its meaning in the *Procura* case.[74] That preliminary reference assessed the compatibility with EU law of the Italian Public Prosecutor's Office's action seeking authorisation to access personal data retained by providers of e-communications services, with a view to identifying the perpetrators of two acts of aggravated theft, robbery, of a mobile phone. In its reference, the *Corte Supreme di Cassazione* said such a provision could give rise to data disclosure requests for "offences with a limited social disturbance and which are punishable only on foot of a complaint by a private party … [for example] low-value thefts such as mobile phone or bicycle theft".[75]

The CJEU upheld the provision in question, clarifying that it is for Member States to define "serious crime" for the purposes of Article 15 of the ePrivacy Directive.[76] It elucidated that Member States "cannot distort the concept of serious offence" by including offences that are "manifestly not serious in the light of the societal conditions prevailing

[70] Ibid., at [149].
[71] Ibid., at [150].
[72] TEU, art. 4.
[73] Judgment of 20 September 2022, *Bundesrepublik Deutschland v SpaceNet A.G. and Telekom Deutschland GmbH*, C-793/19 and C-794/19, EU:C:2022:702 (hereafter, "S*paceNet*").
[74] Judgment of 30 April 2024, *Procura della Repubblica presso il Tribunale di Bolzano*, C-178/22, EU:C:2024:371.
[75] Cited in ibid., at [21].
[76] Ibid., at [46].

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

in the Member States concerned".[77] To avoid the dilution of the concept of "serious crime", the CJEU held that access requests must be subject to prior review by a court or independent administrative body with the power to refuse or restrict access where the crime is not serious.[78]

D. Practical Considerations: Proportionality and Necessity

The 2013 Edward Snowden revelations implicated state intelligence agencies in intercepting and monitoring the data flowing through submarine cables in far-reaching critical surveillance practices. Should privacy become the by-word for apex courts as a hierarchy of objectives emerges, with the victims of crime exacting the highest price? The resolution of that question has been an unending job for national courts. The preliminary reference procedure found in Article 267 TFEU has a role here as the tool for judicial dialogue between national and supranational courts. The supposed dialogue, however, has been criticised by the Supreme Court of Ireland as "rather one-sided".[79] Proportionality, as a theoretically "rigorous, standard based doctrine" that aims to mitigate against subjectivity "inherent in the exercise of power", is the reputed safeguard.[80] In reality, proportionality has implied the exercise of a value judgment in placing metadata exclusion over all other interests.

Practicality matters. On what evidence is it postulated that terrorist crime is more of a threat, hence justifying interference with privacy, than serious crime? There is no basis for believing that the entire foundation of police work grounded upon the build-up of suspicion could be forced through the opposite lens of prediction. On this logic, the *Procura* decision invites double criticism. First, it begs the question of whether the CJEU's approach distorts privacy rights or whether it invites Member States to re-categorise singular investigations. That appears the response of the Italian legislature. Second, the CJEU's emphatic rejection of the relevance of the metadata belonging to a pre-identified criminal – as in the minor thief – to the proportionality test necessary for lawful access to metadata seems to be the antithesis of both the targeted retention model and the public nature of crime. Crime is not a private matter. This principle informs the prosecution of all criminal offences. This is

[77] Ibid., at [50].

[78] Ibid., at [60]. Prior to this ruling, Article 132(3) of Italian Legislative Decree No. 196/2003 was amended to classify offences for which telephone records may be obtained as "serious", punishable by at least three years imprisonment. As to the criteria for assessing the existence of a serious interference with the rights guaranteed in Articles 7 and 8 of the Charter, the court held, at [41], the "fact that the data to which the Public Prosecutor's Office requested access may not be the data of the owners of the mobile telephones at issue, but the data of the persons who communicated with each other by using those telephones after their alleged theft, is irrelevant".

[79] *The People (D.P.P.) v Caolan Smyth* [2024] IESC 22, [2024] 6 J.I.C. 1705, at [97] (Collins J.).

[80] L.D. Corte, "A Critical Comment on Proportionality in the Mass Surveillance Jurisprudence of the CJEU and the ECtHR" in Kosta and Kamara (eds.), *Data Retention*, ch. 4.

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

demonstrable. The 1996 Veronica Guerin murder case (Section III (A)), the 1998 Omagh bombing (Section III (A)) and the 2015–2024 Graham Dwyer murder prosecution (Section III (D)), are articulated below to demonstrate the CJEU's approach as a contradiction of fact.

The decision in *Digital Rights Ireland* is the inaugural wrong-turning. There, the court assessed proportionality considering the Directives' main object, namely crime prevention, and not its stated objective, that of market harmonisation; sitting uncomfortably with its finding in *Ireland v European Parliament and Council of the European Union*. It is also evident, that the CJEU has not treated all types of retained data in the same way. In addition to the terrorist and (highly qualified) serious crime exceptions – noting the differing tests for each – and the preclusion of the mass harvesting of data, Internet piracy has recently generated another exception. In the *French Data Network* case,[81] the CJEU considered a referral seeking an annulment of a French decree which authorised the public authority responsible for the protection of copyright and related rights infringements committed on the Internet to access data, retained by service providers. The processing operation at issue enabled the matching of the civil identity associated with the Internet Protocol (IP) address that appeared to have been used for copyright infringement, without prior review by a judge or independent authority. Offenders faced a graduated response; educational to punitive measures or, in the most serious cases, a referral to prosecution.

The court held that access by a public authority to data relating to the civil identity associated with an IP address retained by providers of electronic communications services was justified under Article 15 of the ePrivacy Directive for the purpose of combatting counterfeiting offences. According to the court's earlier case law, IP addresses constituted traffic data for the purposes of the ePrivacy Directive. However, in grafting an exception in support of intellectual property law enforcement, the CJEU held that "[IP addresses] are distinct from other categories of traffic data and location data … [and they] … mainly serve to identify … [the owner] of the terminal equipment from which a communication is made".[82]

Thus, the court enabled scrutiny of email and Internet telephony, "provided that only the IP address of the source of the communication are retained and not the addresses of the recipient of the communication, those addresses, do not, as such, disclose any information about third parties who were in contact with the person who made the communication".[83] Yet, on the same point in *La Quadrature du Net* the court considered that IP

[81] Judgment of 30 April 2024, *La Quadrature du Net and Others v Premier Ministre, Ministère de la Culture, French Data Network and Others*, C-470/21, EU:C:2024:370 (hereafter, "*French Data Network*").
[82] Ibid., at [75]–[76].
[83] Ibid., at [76].

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

addresses "when used to track an Internet user's complete clickstream and therefore his or her online activity, enable a detailed profile of the user to be produced … therefore retention and analysis of those IP addresses … constitute a serious interference with fundamental rights of the internet user".[84] Puzzling is the emphasis the CJEU attached to effective criminal investigation and to the fact that, absent access to the data, there would be a "real risk of systemic impunity" not only for copyright infringement but for other offences committed online or "facilitated by the specific characteristics of the internet".[85] From the outset, it is difficult to justify the level of gravitas the decision seems to attach to the detection of crime committed exclusively online compared with the preponderance of illegal activity which has online and offline elements. The decision also emerges as contradicting earlier case law where the court held that while indiscriminate retention of data is permissible, it requires the crime to have a certain degree of seriousness, which usually does not apply to infringements of copyright online.[86]

According to the court, Member States must lay down, in its legislation, clear and precise rules relating to retention arrangements associated with IP addresses, which must meet strict requirements:

- The national rules must ensure that each category of data, including data relating to civil identity and IP addresses, "is kept completely separate from the other categories of data retained".[87]
- Those rules must "ensure that, from a technical point of view, the separation of the various categories of retained data was genuinely watertight, by means of a secure and reliable computer system".[88]
- As far as the rules provide for the possibility of linking the retained IP addresses with the civil identity of the person concerned, "the rules must do so through the use of an effective technical process which do not undermine the effectiveness of the watertight separation of those categories of data".[89]
- The reliability of "that watertight separation must be subject to regular review by a public authority other than that which sought to obtain access to the data".[90]

As the CJEU isolates one type of metadata from intrusion in the context of copyright infringement, almost invariably pursued as a civil wrong, but as a crime it is much less serious than the abuses inflicted on victims by sexual

[84] Judgment of 6 October 2020, *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, at [153].
[85] Judgment of 30 April 2024, *French Data Network*, C-470/21, EU:C:2024:370, at [119].
[86] Judgment of 6 October 2020, *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, at [46].
[87] Judgment of 30 April 2024, *French Data Network*, C-470/21, EU:C:2024:370, at [86].
[88] Ibid., at [87].
[89] Ibid., at [88]
[90] Ibid., at [89].

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

and other forms of violence and by major thefts. The position that the disclosure of identity of the user in the absence of profiling does not constitute a serious interference with Charter rights is difficult to reconcile with the CJEU's previous case law that explicitly states that disclosure of traffic and location data is a serious interference of Charter rights.

In *G.D. v Commissioner of An Garda Síochána and Others*[91] – prosecuted in Ireland as *The People (D.P.P.) v Graham Dwyer*[92] – the CJEU rejected the Commission's argument that particularly serious crime could be treated in the same way as threats to national security. The Court referred to its earlier case law outlining a hierarchy of public interest objectives that may justify restrictions to rights protection according to their respective importance. Such a measure must be proportionate to the seriousness of the interference that it entails.[93] By allowing broader exceptions to the principle of data minimisation, the CJEU seems to have undermined its own rationale for avoiding the dilution of the concept of "serious crime" posited in *G.D.* and *SpaceNet.* The result of the proportionality test in the context of copyright enforcement is the converse of what the CJEU had determined as unconstitutional;[94] previously the court held that data disclosure and retention requests by public authorities require prior review.

This decision seems to invite inconsistent degrees of protection from intrusion to privacy for criminals and mercenaries alike. According to one report, Member States' responses to the development of CJEU jurisprudence have been met with reluctance and a diversity of approaches by national governments.[95] In the fog generated, a map is needed. The metadata regulatory framework across the EU for Member States can be summarised as follows:

- Member States in which the domestic legislation implementing the Data Retention Directive remains in force;
- Member States which amended their legislation or enacted new data retention laws in line with the CJEU case law. 12 counties made changes to their legislation in the period from 2018 to 2022, seven of which introduced targeted retention. For example, in Ireland, for national security purposes, the Communications (Retention of Data) (Amendment) Act 2022, requires all telecommunication service providers to retain metadata for a period of 12 months from the date on which the data were first processed by the service provider;

[91] Judgment of 5 April 2022, *G.D. v Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258 (hereafter, "*G.D.*").
[92] *The People (D.P.P.) v Graham Dwyer* [2024] IESC 39, [2024] 7 J.I.C. 3116 (hereafter, "*Dwyer*").
[93] Judgment of 5 April 2022, *G.D.*, C-140/20, EU:C:2022:258, at [56].
[94] G. Westkamp, "Data Retention, Information Disclosure and Intellectual Property Enforcement: A Truly 'High Standard' of Protection?" (2025) 1 Intellectual Property Quarterly 48.
[95] European Commission, *Final Report*, 25.

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

- Member States whose national laws transposing the Data Retention Directive were struck down and which now lack any metadata retention laws.

III. Current Position

On the protection of data, on its exceptions and on the judgments supporting the approach of the CJEU as justifying its rulings, there is a thicket of case decisions. From these, it is barely possible to discern the current position. While this may not be final, what follows may assist as a workable taxonomy:

(1) EU law precludes general and indiscriminate retention of traffic and location data by providers of electronic communication services; *Digital Rights Ireland*.[96] Hence, bulk data retention is incompatible with EU fundamental rights, even if it is accompanied by a strict access regime, mediated through a judge or other independent person; *Tele2* confirmed in *SpaceNet*.[97]

(2) To combat non-terrorist or non-state-threat crime, EU law precludes general and indiscriminate retention of traffic and location data. Targeted retention is permitted, only by predicted geographic area or expedited retention through the pre-identification of a person on the basis of objective evidence (quick freeze); *Tele2*.[98] There may be different levels of interference that require additional or less justification; *Ministerio Fiscal*.[99] These findings, uncertainly, are not perhaps applicable to subscriber data.[100]

(3) However, EU law allows general and indiscriminate retention of traffic and location data by providers of electronic communications services to safeguard national security. This can be intuited to cover, most obviously, terrorism or risk of invasion, surely including cyber-attacks. Here a set of considerably more flexible conditions are to be met. These do not require a prior reasonable suspicion focused on individuals or focused on geographic areas. The retention must be "time limited" and there must be "sufficiently solid grounds for considering that the Member State concerned is confronted with

[96] Judgment of 8 April 2014, *Digital Rights Ireland*, C293/12, EU:C:2014:238.
[97] Judgment of 20 September 2022, *SpaceNet*, C-793/19 and C-794/19, EU:C:2022:702.
[98] Judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970.
[99] Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2022:702 (hereafter, "*Ministerio Fiscal*").
[100] European Council, "Document 14319/18", available at https://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf (last accessed 27 July 2025). While Member States broadly agree on what constitutes metadata, some classify points such as IP addresses and device identifiers as subscriber data, others as traffic data.

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

a serious threat … to national security which is shown to be genuine and present or foreseeable"; *La Quadrature du Net*.[101] The data must be liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment used; *Prokuratuur*.[102]

(4) However, as a further exception, EU law allows general and indiscriminate retention of IP addresses to match the civil identity data of its holder to detect copyright, or perhaps similar infringements of intellectual property on the internet, once certain requirements are met, without prior review by a judge or independent authority, save for "atypical situations" that are likely to reveal sensitive information; *French Data Network* case.[103]

This line of cases, generated the ultimate decision on the legality of bulk data retention; *G.D. v Commissioner of An Garda Síochána and Others*.[104] These facts are taken from the prosecution narrative.[105] The victim met the accused and, over time, he increasingly expressed a desire to violently abuse women. He was a professional with no convictions. His wide professional travel exposes the invalidity of supposed geographic targeting. The police discovered a number of mobile phones, which they claimed to connect to the accused and others of which relatives linked to the victim. Analysis of messages on these revealed violent fantasies. As part of the investigation, the accused was known to have travelled to certain places on particular dates and the mobile phones were ascribed to him by recovered metadata based on his proven presence in, or declared intention to be at, particular places. Hence, having first ascribed the phones to the victim and accused, a request was made to a police officer, not a judge, for relevant raw metadata to be accessed and analysed. This, it was claimed, established both a pattern which enabled identification of the accused, thus furthering the central tenet of acquaintance between the victim and accused, and motive and inclination. In a preliminary ruling as to admissibility, the Supreme Court of Ireland submitted questions to the CJEU as to whether the metadata of the accused had been illegally harvested by investigators.[106] This would have a serious bearing on the

[101] Judgment of 6 October 2020, *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791.

[102] Judgment of 2 March 2021, *H.K. v Prokuratuur*, C-746/18, EU:C:2021:152; see also judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2022:702.

[103] Judgment of 6 October 2020, *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, at [134]–[135].

[104] Judgment of 5 April 2022, *G.D.*, C-140/20, EU:C:2022:258.

[105] Note that the authors express no view as to the validity of such assertion or as to any legal proposition debated.

[106] *Dwyer v The Commissioner of an Garda Síochána* [2020] IESC 4, [2020] J.I.C. 2401, at [7.2] (Clarke C.J.). In the final analysis, although this data was accessed illegally, the court applied a principle that

admissibility of this key evidence. A central issue for the Irish Supreme Court was whether the trial judge was correct to admit the telecommunications data of the accused. The CJEU reaffirmed, in absolutist terms that "there can be no question of reinstating ... the general and indiscriminate retention of traffic and location data"[107] and "the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into the rule, to provide for general retention of traffic and location data".[108]

A. Sense and Sensibility?

Law should be based on good sense. Organised crime, as in the Veronica Guerin murder, can be as much an attack on society as such terrorist acts as the Omagh bombing. Both prosecutions relied on harvested telecommunications data as key evidence. Apart from that, the victims of serious crime should have an equal right to court processes which have access to a category of proof which experience has shown to be compelling. Two contrasting cases demonstrate the centrality of metadata in combatting all forms of crime. Hence, we briefly reference the murder of a journalist in Ireland by organised crime and the murder of those in Omagh, within the UK jurisdiction, by terrorists. The first victim died while investigating organised crime and the second set of victims perished due to warped ideology. All, however, are victims: in one category the CJEU's reasoning would now undermine a vital investigative instrument. In neither case was any private information about non-suspects ever revealed or any complaint of intrusion ventilated.

In June 1996, Veronica Guerin, was shot, while stopped at traffic lights near Dublin city, by members of a gang she was investigating. She had been tracked by her killers travelling away from Dublin and then followed on her journey and murdered while returning. The perpetrators were a Dublin gang, importing drugs and automatic weapons. Of the seven main participants, one was ex-army with no convictions (no reason to predict criminality), another was running a shipping company in Cork (similarly) and another was unemployed and had no convictions (similarly). The other four had convictions for serious offences, but years previously, with no current police suspicions. The CJEU's position suggests that the prediction of crime, enabling the targeting of telecommunications data, can lawfully be retained and harvested only by augury. As to proof, at trial a pattern was established of the phones of gang members communicating with each

where the law had changed, this could not be regarded as such an egregious breach of the rules of evidence to require exclusion. The problem, however, is with future cases.

[107] Judgment of 5 April 2022, *G.D.*, C-140/20, EU:C:2022:258, at [83].

[108] Ibid., at [84].

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

other. Locations and interactions established involvement in the crimes.[109] This was harvested from the incomprehensible data as to which phone communicated with which other phone, for how long and with which mast the caller and the receiver's phones connected. Since there was no surveillance of the words spoken but only by targeted deciphering of commercially retained information, it is difficult to see how privacy rights would be engaged. Even if engaged, the derogation for the investigation of murder both serves and is proportionate to a legitimate aim.

On 15 August 1998 in Omagh, Northern Ireland, a bomb was exploded killing dozens and injuring multiple other victims. The mobile phone of the person accused of conspiring to perpetrate the bombing was analysed and its metadata was recovered pursuant to the safeguards under Irish and British legislation. By a ruse, a second mobile phone, that of an uninvolved man, was borrowed. There was no reason to suspect the uninvolved man of being complicit. The metadata showed the two phones communicating in a pattern of staccato calls from Dundalk to Omagh (a distance of 110 kilometres) and returning on the same route. This established an advancing spotter car, using one phone, and the following explosives-packed car where another mobile received warnings on security checks. Analysis produced no convincing reason for this kind of pattern where the phones utilised masts internationally up and back in a northwest–southwest axis over a short timeframe. This had nothing to do with airports or train stations;[110] geographical prediction being demonstrated to be unreal. The traffic was international, and hence impossible for prior geographical targeting. The phone communicating from the spotter car travelled about 1.5 kilometres ahead of the car which had been turned into a bomb. The calls were routed through fixed masts, showing a pattern. The Special Criminal Court regarded this evidence as central to the conviction in the case of *The People (D.P.P.) v Colm Murphy*:

> The pattern of calls and sell-mast user by both phones on [the day of the Omagh bombing] indicate that each travelled from County Monaghan [in a Northerly direction] to Omagh shortly before the detonation of the car bomb there and also returned [in a southward direction to County Monaghan where the accused lived] thereafter. It is highly probable that the conveyance of the car-bomb to Omagh that day would have involved, not only the bomb carrying vehicle itself but also a scout car to travel ahead of it. Telephone contact between both vehicles in such circumstances is probable.[111]

[109] See *The People (D.P.P.) v Meehan* [1999] 7 J.I.C. 2901 (S.C.C.), *The People (D.P.P.) v Gilligan* [2005] IESC 78, [2005] 11 J.I.C. 2301.

[110] Judgment of 6 October 2020, *La Quadrature du Net*, C-511/18, C-512/18 and C-520/18, EU: C:2020:791, at [152].

[111] *The People (D.P.P.) v Colm Murphy* [2002], judgment of 22 January 2002, not reported (S.C.C.). Note that this decision was overturned on appeal due to a legal error made by the trial court; see *D.P.P. v Murphy* [2005] IECCA 52, [2005] 4 I.R. 504.

B. Evidence and Exclusion

The law of evidence evolved through experience but fundamental is that "the law is entitled to the evidence of every man".[112] Common sense suggests the search for the truth is most likely to yield results when a court receives all available, relevant information. Jeremy Bentham wrote of the judicial system that it was one of "free proof"[113] – in which evidence was admitted if logically relevant. Rules of exclusion, however, inform the archetype of every legal principle's inception. In civil law systems generally, the tribunal should "admit any evidence which it deems to have probative value", leaving the weight as a matter for analysis.[114] Some sources of exclusion of evidence in common law originate in the fragility of jury analysis. But, in addition, social considerations require some sources of evidence to be exempt: hence, privilege. Outside of proof in court, common law protects categories of evidence from harvesting, the classic example being that lawyers giving advice to clients are bound to confidentiality. Here there is sense. As analysed by Wigmore, privileged communications should be protected from admission in evidence where a relationship of confidence is inherent in the transmission of information, where society has an interest in protecting that form of relationship (e.g. lawyer and client) and where undermining the secrecy of that relationship would cause greater damage to social cohesion than removing the information in the communication from its reception as evidence.[115]

Nullifying an entire category of proof undermines the judicial system. The human rights of victims are subject to privacy concerns; in contrast to the logic behind privilege, a much lesser concern. Further, there is no distinction to be found in classifying the form of proof that is possible and the kinds of investigation into violations that may be pursued, between what is ordinary crime and a taxonomy of offences based on undermining the nation state. Intellectual property protections, while justified, are not superior to the right to life. The nation state exists to foster common values, one of which is the protection of those within the jurisdiction of its borders and laws.

In EU law, proportionality is central to every limitation on fundamental rights and is applied through the limbs of suitability or appropriateness and

[112] *The People (D.P.P.) v J.T.* (1998) 3 Frewen 141 (Circ. Ct. (Crim.)).

[113] J. Bentham, *Rationale of Judicial Evidence, Specially Applied to English Practice*, vols. 1–5 (London 1827), 209.

[114] G. Williams, *The Proof of Guilt: A Study of the English Criminal Trial*, 3rd ed. (London 1963), 208. Article 1358 of the French Civil Code "except where the law provides otherwise, proof may be provided by any means". Similarly, Article 286 of the German Civil Code allows a court to analyse any evidence, but it must give reasons as to why it finds evidence probative.

[115] J.H. Wigmore, *A Treatise on the Anglo-American System of Evidence in Trials at Common Law*, 3rd ed. (Boston 1940).

through the test of necessity.[116] The prevailing case law of the CJEU has misstated the proportionality assessment to which interferences with the fundamental right to protection of personal data operate at a stratum where vital evidential proof is nullified.

Central to compliance with proportionality are the strict necessity test and the appropriateness test. The strict necessity threshold as applied to the overall proportionality test has been so strained as to become unpredictably applied. This flows from the court's conflation of the necessity for a measure with the final element of the test: strict proportionality. This is "the part of the test where competing rights, or rights competing with objectives of general interest worthy of protection, are balanced against each other".[117] The balancing test as applied to data preservation, production and disclosure orders lacks satisfactory resolving power to the competing interests at stake.

That emerged from one of the earliest interpretations of the application of proportionality to this issue in the opinion of Advocate General Saugmandsgaard Øe in *Tele2*. The advocate general stated that "the requirement of proportionality within a democratic society prevents the combatting of ordinary offences and the smooth conduct of proceedings other than criminal proceedings from constituting justifications for a general data retention obligation".[118] Later case law, as analysed, divining exceptions to that principle, reveals a complex taxonomy of objectives allowing different degrees of metadata retention that do not equate to the degree of criminality at issue.

C. Privacy

If the EU yields to a position where rights of general application enacted in aid of privacy are capable of thwarting criminal investigations, it requires an analysis of the origin of the weight the CJEU affords to privacy. *Scarlet Extended S.A. v Société Belge des Auteurs, Compositeurs et Editures*[119] provided a hint that the CJEU might move in the direction of an almost absolute determination to establish and preserve anonymity for electronic data use. The decision arose from a 2004 request by the Belgian Association of Authors, Composers and Publishes for an order from the Belgian court requiring Scarlet, an Internet service provider, to prevent copyright infringements committed through its service by blocking customers from sending or receiving files contained in protected works. The Belgian court found in favour of the authors' group, but the CJEU

[116] D. Nardi, "Proportionately and Strict Proportionality in the Case-Law of the Court of Justice of the European Union on Data Retention" in Kosta and Kamara (eds.), *Data Retention*, ch. 5.
[117] Ibid., at 64.
[118] *Tele2 Sverige v Post-och Telestyrelsen* [2017] Q.B. 771, at [172] (Saugmandsgaard Øe A.G.)
[119] Judgment of 24 November 2011, *Scarlet Extended S.A. v Société Belge des Auteurs, Compositeurs et Éditures S.C.R.L.*, C-70/10, EU:C:2011:771.

rejected that interpretation, stating that the installation of a filtering system may infringe the right to protection of the personal data of Internet service provider's customers.[120]

Yet, privacy is a highly fact-dependent right. There may be situations of confidence, through commercial or personal relationship, were privacy rights demand protection. Conversely, a state of affairs commonly occurs where legislation-based rights may apply but where there can be no reasonable expectation of non-disclosure, for example arranging a serious crime. But, in any of these, statutory obligations may superimpose a blanket constriction. In the field of communications, the legislative model is that data may only be retrieved in accordance with law and when authorised. The very fact of restricting that kind of evidence, in distinction to documentary or eye-witness testimony, makes the interpretation of legislative norms one that demands shrewd and reality-based analysis by an apex court.[121]

D. Human Rights

Critics may see human rights as asserting protections for those accused of crime. Those who have suffered a criminal violation also have rights. Without the secure retention of metadata and the potential to access and analyse it for strictly limited purposes related to criminal investigation, the most serious crime has a much greater chance of remaining undetected. Cutting out the truth in the form of key evidence distorts the legal process and severs it from good sense. Arguably, the European Court of Human Rights ("ECtHR") has struck this balance proportionately.[122] In *KU v Finland*, the ECtHR explicitly held that "[a]lthough … users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee[s] cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others".[123]

In the wake of these cases, just how much criminality society is willing to tolerate in pursuit of a particular conception of protection of proclaimed freedoms will have to be reckoned with. In consequence of the CJEU's decision in *Norra Stockholm Bygg*,[124] the question over the use of metadata in civil proceedings is on an equal, but no less expansive,

[120] Ibid., at [50]–[51].
[121] P. Charleton and S. Reilly, "Passing Off: An Uncertain Remedy" in European Union Intellectual Property Office (ed.), *20 Years of the Boards of Appeal, Celebrating the Past, Looking Forward to the Future Liber Amicorum* (EUIPO 2017), 136.
[122] O'Leary, "Balancing Rights".
[123] *KU v Finland* (Application no. 287/02), Judgment of 2 March 2009, not yet reported, at [49].
[124] Judgment of 2 March 2023, *Norra Stockholm Bygg A.B. v Per Nycander A.B.*, C-268/2, EU:C:2023:145 (hereafter, "*Norra Stockholm Bygg*").

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

trajectory to that followed in the criminal law. Those proceedings confirm the application of the GDPR to civil court proceedings, including court orders to produce documents containing personal data as evidence. When assessing the production of a document containing personal data, the national court is required to have regard to the interests of the data subjects and balance these on a case-by-case basis, considering the type of proceeding at issue and taking into account the principle of proportionality and data minimisation (the last resort principle whereby evidence by other means should be pursued rather than retained data). As real evidence, the law's treatment of banking data provides an extreme point of comparison to the data-nullification debate. In common law, what was known as the "best evidence rule" possibly originated through judges noticing mistakes in hand-copying documents. The rule that proof must generally be offered by producing the original has weakened in favour of an analysis as to the weight to be afforded to a copy. But banking data, evidenced by the use of a credit card system that a customer spent a certain amount in a location on a particular date, proves both presence and potentially reveals more as to proclivities. This data might more properly be protected by privacy rights. Yet, here, proof is thus far unimpeded.[125]

IV. Conclusion

While there are dangers in placing privacy on the lowest rung of any taxonomy of rights, using digital privacy as a norm that nullifies crucial evidence overrides the entitlement of the victims of serious crime to a fair judicial process. The CJEU asserts that by retaining data there is a risk of abuse and unlawful use.[126] Yet, the CJEU's blanket data retention ban in the fight against serious crime threatens social cohesion. Arguably, the global trade in information, facilitated by policies such as the EU's Digital Agenda, under which the European strategy for data has been central,[127] may threaten privacy more than time-limited retention for law enforcement purposes.[128] Under the placate surface of privacy rights lies the offering serious criminal offenders typically find most enticing; anonymity. Fundamentally, the admissibility of evidence in court is a matter for the judge presiding over litigation and while the various decisions of the CJEU do not change that principle, the case law divests

[125] Usually, retention periods for personal data are outlined by legislation, with the GDPR derogating the decision to data controllers.

[126] Judgment of 5 April 2022, *G.D.*, C-140/20, EU:C:2022:258, at [45].

[127] The European strategy for data explicitly states that it will "ensure that more data becomes available for use in the economy and society"; see "A European Strategy for Data", available at https://digital-strategy.ec.europa.eu/en/policies/strategy-data (last accessed 10 December 2024).

[128] As may be the transfer of data under the Safe Harbour Agreement, see Judgment of 6 October 2015, *Maximilian Schrems v Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650. If not available in Europe, perhaps the information being transferred minute by minute to the US may be requested.

judicial authority. The deficit in the apodixis of the various judgments might be seen as removed from reality of the paradigmatic cases of Omagh, *Dwyer* and Guerin. These are not untypical of what can happen anywhere.

The "golden thread" weaving through the criminal law is the duty of the prosecution to prove an accused person's guilt.[129] For proof in civil and criminal litigation, metadata should be available. It is the stringent protection of privacy in the form of data, as a CJEU-declared supreme interest,[130] that threatens the principle of finding the truth. This two-step of balancing rights yet also finding the truth, common to all court proceedings, requires flexibility. Yet, arguably, it has become unworkable where harvesting telecommunications data for evidence is concerned. The exclusion of evidence relating to harms attracting a high degree of culpability in furtherance of a particular conception of privacy protection lacks a foundation in reality. To this seemingly compromised system of justice, there are exceptions divorced from reason and logic. Thus, the victims of crime have been trumped by privacy. The trajectory of case law since *La Quadrature du Net* has been one of case-by-case exceptions to the CJEU's general retention prohibition. These do not follow from the principle, emerging as post-hoc rationalisations perhaps designed to avoid the logical consequences of *Tele2*.

As highlighted by the Supreme Court of Ireland, the implications of that dismissal of general data retention, "is far from obvious from the language of Article 15(1) of the ePrivacy Directive or of the Charter and appears to be highly contestable".[131] Civil litigation might be regarded as less important: but not to those seeking justice. Furthermore, experience in Ireland and in the UK demonstrates, first, that terrorist activities often involve money laundering, bank robbery, fraud or other forms of theft, drug dealing and the illegal importation of weapons. These also are individual crimes. Second, unchecked organised crime can grow so menacing as to threaten state security; in which case, the CJEU's distinction becomes meaningless. While EU institutions have tended to define "national security" narrowly, this kind of uncertainty strikes at the constitutional heart of the rule of law.

As to the lawful interception of data in pursuit of serious crime, the alternative models of targeted data retention posited by the CJEU are not based on experience; but emerge as unworkable and impractical. Digital evidence can play a key role in 85 per cent of major criminal investigations.[132] Prior authorisation for inert data storage could not have

[129] *Woolmington v Director of Public Prosecutions* [1935] A.C. 462, 481 (Viscount Sankey L.C.) (H.L.).
[130] C. Kuner, "A 'Super-Right' to Data Protection? The Irish Facebook Case & the Future of EU Data Transfer Regulation", available at https://blogs.lse.ac.uk/medialse/2014/06/24/a-super-right-to-data-protection-the-irish-facebook-case-the-future-of-eu-data-transfer-regulation/ (last accessed 2 May 2025).
[131] *The People v Caolan Smyth* [2024] IESC 22, at [95] (Collins J.).
[132] European Commission, *Commission Impact Assessment on Proposals for a Regulation for Electronic Evidence in Criminal Matters and a Directive on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings* (Brussels 2018).

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

solved the Guerin or Omagh murders, with several suspects beyond suspicion. As to geographical range, this would involve guesswork. Two jurisdictions and several towns were involved in the Omagh outrage, and Dublin, Kildare and Cork were the random locations that the relevant crime scenes threw up in the murder of the journalist. It was because of travel of the suspect that the data in *Dwyer* became significant. Criminals do not advertise themselves (prior suspicion) or house themselves in groups (geographical targeting). Nor are their activities limited to transport hubs such as airports.

Quick freeze, the posited universal solution of the CJEU, is ill-suited to crimes committed via electronic means and to those which raise cross-border issues. One thinks of sexual exploitation or cyberattacks or complex organised criminality, often detected much later. Some 3,892 requests for communication data were made as part of Operation Notarise, an investigation carried out by the UK National Crimes Agency which resulted in the arrest of 660 suspected paedophiles who had been viewing perverted images of children. 3,982 requests for communications data were made as part of this operation, of which, 92 per cent were able to be resolved to identify a suspect.[133] A further deficit to quick freeze is that expedited retention can only be applied from the moment a crime is detected or, more rarely, suspected and it relies on the happenstance of data actually being stored by electronic service providers.[134] The viability of the targeted retention model is less than certain given that some Member States do not have a legal obligation on electronic service providers to retain metadata. Some crimes committed online, therefore, may not be detected at all or until years later. Excluded, in terms of the availability of metadata for effective and thorough investigation, are the victims of unsolved crimes and of missing persons, the bodies of whom may turn up years afterwards. There is evidence that criminals are increasingly taking advantage of privacy protecting measures.[135] Experts point out that accessing data may also be important to exonerate a suspect and to protect the rights of a defendant. Others have said that the court's criteria are "problematic with respect to fundamental rights because of discrimination against categories of persons or location".[136]

Practical problems associated with targeted retention proliferate. In some cases, companies do not provide information on the specific data they

[133] Anderson, *Question of Trust*, at [7.51].

[134] C. Dupont et al., "Study of the Retention of Electronic Communications Non-Content Data for Law Enforcement Purposes: Final Report", available at https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71a1 (last accessed 29 July 2025).

[135] "Concluding Report of the High-Level Group on Access to Data for Effective Law Enforcement", available at https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf (last accessed 4 December 2024).

[136] "Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement 2024", 8, available at https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en (last accessed 4 December 2024).

process and hold, rendering it difficult for competent authorities to submit targeted data access requests.[137] Implementation problems are emerging because some of the CJEU's retention criteria were based on technologies that have evolved since the judgments were issued.[138] Studies suggest metadata evidence can compensate the administration of justice for evidence lost due to encrypted communications.[139] Hence, before making legal pronouncements of broad-sweep, courts of final authority should consider the unintended consequences of what may then appear as attractive.[140] This impacts on the ability of law enforcement authorities to uphold citizens' rights and is particularly alarming given the emphasis placed by the CJEU in *G.D.*[141] and in *SpaceNet*[142] on the availability of targeted retention as a way forward on data retention and in mitigating the negative effects of the unavailability of general retention, despite the evidence-based findings of the Irish Supreme Court in *Dwyer* that such measures would not be effective.[143]

All in all, the obligation of the right to life, enshrined in Article 2 of the Charter, cannot propose that a life taken by reason of terrorism is worthy of a more cogent level of proof than a life taken as a result of criminal activity for personal gain or through acting out warped fantasies. This ever-quickening tangle potentially fuels a constitutional struggle between EU institutions and Member States; arguably laying down a crumbling basis, inimical to certainty in the law, for proof in civil and criminal litigation.

The flaw of the CJEU's analysis is to deem privacy as a goal worthy of limiting an investigative tool and vital evidential proof. Proportionality, in its most extreme application is degraded and promotes data minimisation at a high social cost. Privacy protections are a legitimate aim of democratic societies. But exceptions to the principle that cogent evidence is admissible evidence must be rational. Where evidence is put beyond use, practical reasons of social utility can justify exclusion from the judicial process. Good sense and long experience constitute a rational foundation, but that is absent here. Hence, our critique lies in the frailties of the CJEU's approach to the proportionality and necessity assessment vital to constraints on the vindication of fundamental rights and freedoms.

The strength of the legal system depends on public confidence in its ability to administer justice. If targeted retention fails, the stringent access requirements cemented by the jurisprudence of the CJEU means

[137] Ibid., at 27.
[138] E.g. Dynamic IP addresses and Carrier Grade Net Address Translation were not developed at the time of the CJEU judgments positing data retention based on geographic targeting; see ibid., at 7.
[139] A.E. Boustead and M.B. Kugler, "Juror Interpretations of Metadata and Content Information: Implications for The Going Dark Debate" (2023) 9 Journal of Cybersecurity 1.
[140] Service providers are alarmed by the costs of the technical implementation of targeted retention and by frequently changing legislation; see "Concluding Report of the High-Level Group", 27.
[141] Judgment of 5 April 2022, *G.D.*, C-140/20, EU:C:2022:258, at [78].
[142] Judgment of 20 September 2022, *SpaceNet*, C-793/19 and C-794/19, EU:C:2022:702, at [112]–[113].
[143] *Dwyer v The Commissioner of An Garda Síochána* [2020] IESC 4, at [4.5] (Clarke C.J.).

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press

that, at worst, and not at all improbably, the availability of potent evidence in the detection of ordinary crime might be at the mercy of the internal policy of an e-communications service provider. A compromised system of justice in favour of an absolute principle above what is known as to human behaviour stifles truth and tends to draw the law away from its fundamental purpose in ordering society.

https://doi.org/10.1017/S0008197325100962 Published online by Cambridge University Press