ARTICLES

FUTURE-PROOF REGULATION AND ENFORCEMENT FOR THE DIGITALISED AGE

Edited by Gavin Robinson, Sybe de Vries *and* Bram Duivenvoorde

TARGETED RETENTION OF COMMUNICATIONS METADATA: FUTURE-PROOFING THE FIGHT AGAINST SERIOUS CRIME IN EUROPE?

GAVIN ROBINSON*

TABLE OF CONTENTS: I. Introduction: data retention and future-proofing. – II. "The Lighthouse for Privacy Rights in Europe"? Past and present CJEU case law on communications data retention. – II.1 Retain in haste, repent at leisure: the legacy of Directive 2006/24/EC. – II.2. *La Quadrature du Net* and *Privacy International*: from crime to national security (and back). – II.3. CJEU guidance on "targeted" retention for serious crime. III. Future-proof data retention. – III.1. How future-proof is the case law? ePrivacy reform and judicial fears of profiling. – III.2 First national "targeted" retention laws: the exception becomes the rule? – III.3. What we talk about when we talk about data retention: tomorrow's metadata and future necessity. – IV. Conclusion.

ABSTRACT: In many countries worldwide, everyone's communications metadata is pre-emptively retained by telecoms and internet service providers for possible later use by the relevant public authorities to combat crime and safeguard national security. Within the European Union, however, for nearly a decade the Court of Justice of the European Union (CJEU) has consistently rejected the pre-emptive "general and indiscriminate" retention of communications metadata for the purpose of combatting serious crime – although its position on safeguarding national security is more nuanced. For crime, the CJEU continues to insist that any retention of traffic and location data be done on a "targeted" basis, leaving the details of any such scheme to the relevant legislator (EU or national). This *Article* discusses the prospect of a return to EU-level data retention from a future-proofing perspective. It does so by summarising the most relevant recent CJEU case law, noting its internal consistency but arguing that its future resilience should not be taken for granted, particularly with the ePrivacy Regulation on the horizon. It offers a first analysis of efforts to implement "targeted" retention in national legal systems. Should any fresh EU legislative proposal on data retention emerge, it is argued that in addition to fully complying with the relevant CJEU standards, it will also be essential

* Assistant Professor, Utrecht University, g.l.robinson@uu.nl.

The Author wishes to thank Lyria Bennett Moses, Virginia Passalacqua and Ton van den Brink for opportunities to test ideas developed for inclusion in this *Article*.

www.europeanpapers.eu

ISSN 2499-8249
doi: 10.15166/2499-8249/683

to gauge the desirability of such a reform in light of technological shifts in the information labelled "metadata", and the intertwined condition that any such harmonising measure must be demonstrably effective over time.

KEYWORDS: communications data retention – future-proofing – CJEU case law – crime prevention – data protection – privacy.

I. INTRODUCTION: DATA RETENTION AND FUTURE-PROOFING

Communications metadata reveals when and where you go online, whom you call, message or email, for how long, how often, as well as when and where you happen to go "in real life". In many countries worldwide, everyone's metadata is pre-emptively retained by telecoms and internet service providers for possible later use by the relevant public authorities to combat crime and safeguard national security.

In its seminal 2014 judgment in *Digital Rights Ireland*, the CJEU noted that metadata is information which, "taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[1] In the follow-up judgment in *Tele2*, the Court observed that it may provide a means "of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications".[2] Memorably, even hauntingly, the Court opined that where users are not informed that "their" retained data has been accessed by the authorities, this is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[3]

As such, blanket metadata retention goes beyond that which is strictly necessary to combat even the most serious crime and violates the rights to respect for private life (art. 7) and data protection (art. 8) enshrined in the Charter of Fundamental Rights of the European Union. No degree of substantive trammelling and procedural tightening could repair it; blanket retention will be unlawful even when a national retention law:

a) restricts access to cases of serious crime

b) strictly limits means of communication affected, categories of data retained and retention period(s),

c) requires prior review of access requests by a court or an independent administrative authority (except in urgent cases),

d) ensures solid data security and storage within the EU, and provides for notification of the person whose retained data has been accessed.

The near-decade since *Digital Rights Ireland* was decided has brought clusters of high-profile terrorist attacks, growing cybersecurity concerns, the unfurling of the GDPR in the

[1] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* ECLI:EU:C:2014:238 para. 37.

[2] 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* ECLI:EU:C:2016:970 para. 99.

[3] *Digital Rights Ireland* cit. para. 37; *Tele2* cit. para. 100.

European legal order, and multiple scandals detailing corruption and abuse of power within law enforcement authorities in EU Member States. As will be seen in II. below, far from rowing back its stance on data retention for the purpose of combatting crime, in the intervening years the judges in Luxembourg have doubled down on their position, as national regime after national regime has been deemed incompatible with the Charter on the grounds that it entails "general and indiscriminate" retention. At the same time, the Court has gone so far as to erect a "hierarchy of public interest objectives" according to which it has confirmed (through gritted teeth) that blanket data retention for the superior purpose of safeguarding *national security* may exceptionally be tolerated.

As the Court's complex jurisprudence expands and is refined through multiple waves of proceedings, it continues to prise open new boxes of questions and challenges affecting actors as far apart as criminal judges and prospective regulators. In Europe, several national governments are now scrambling to piece together domestic data retention schemes that might avoid (further) censure from the CJEU whilst sating the consistent demands of law enforcement for a workable solution to secure the supply of data which is purportedly the lifeblood of today's criminal investigations. Meanwhile, some national criminal justice systems are still bridling at the perceived audacity of the Court and refusing to fully heed its guidance, whilst some national governments seem to favour triggering a direct clash with the case law – extending to challenging the primacy of EU law itself. Potentially at stake, therefore: nothing short of the credibility of the CJEU as a supranational authority on fundamental rights protection.

Against that turbulent backdrop, this *Article* has two goals. The first is to provide, in II., an up-to-date summary and critical discussion of the main legal complexities and contentions running through the now-mature "data retention debate" in the EU. As the first main part of the *Article* aims to show, that maturity need not bring a staleness or stasis, despite a recurrent framing of the debate – especially in mainstream media coverage but also in EU policy circles and academic literature – within the reductive paradigm of a "privacy v security" zero-sum game (more privacy necessarily equals less security, and vice versa). Indeed, the legal tensions generated by the data retention question continue to evolve, whether in the technical (and increasingly, technological) details of the interplay in CJEU case law between fundamental rights standards and national security or crime prevention imperatives, in the friction between shifting visions of national prerogatives and EU competences, or in intensifying dialogue between European and national courts.[4]

Having thus set the scene in II. with a snapshot of the EU data retention debate in 2023, in keeping with the future-proofing theme of this special issue the *Article*'s second goal is to look forward: ultimately, to the prospect of "data retention 2.0" – a fresh

[4] J Podkowik, R Rybski and M Zubik, 'Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?' (2022) ICON 1597.

proposal for EU legislation on the matter.[5] Will we see such a proposal soon? In III., this *Article* seeks neither to predict future policy developments nor – in the limited space available here – prescribe specific criteria for future-proof legislation on data retention (whether at EU or any national level).[6] It also eschews assuming a normative stance as to whether a fresh EU data retention law is on the whole desirable. Rather, it aims to identify priorities for the policy and research agenda for the years ahead, which, it is posited, double as essential prerequisites for any re-introduction of an EU-level data retention mandate that is to be sufficiently resilient, adaptable, durable and legitimate.

For Ranchordás and van 't Schip, "a future-proof approach should be embraced with caution and should primarily entail that legislation takes into account the needs of future generations, remains adaptable and does not entrench politically sensitive policy programmes or institutions".[7] The same authors examine the potential of two instruments for the implementation of their proposed future-proof approach: "experimental" legislation and future-proof impact assessments.

Viewing the data retention debate in Europe through such a prism is admittedly subject to limitations. The scope for "experimentation" with a view to future-proofing legislation is narrower in issues of criminal law enforcement, which directly connect to public safety. Crime equals real victims, for whom there can be no regulatory sandbox. In the context of "outsourced" surveillance of metadata for public purposes, room for norm flexibility is also limited: is a private entity legally bound to retain data or not? What data precisely, and for how long? For what purposes are those data retained, and what kinds of procedural safeguards should govern investigators' access thereto? In such matters, legal certainty weighs heavily in the scales against adaptability.

Notwithstanding these limitations, in III. the *Article* argues that a future-proofing perspective on the data retention debate in the EU is worth taking for three reasons.

Firstly, any future initiative at either EU or national level will have to comply with the CJEU's interpretation of Charter rights, now and into the future – although it will be argued that the Court's position may itself be less "future-proof" than it currently appears and

[5] It is thus possible future regulation aiming to contribute to the fight against serious crime that is the object of future-proofing, and not any sense of future-proofing society itself against serious crime. Indeed, the imperative of crime *prevention* might be seen as a form of future-proofing, in the sense of the progressive calibration of a safer society with ever-fewer instances of (serious) crime. The same notion might apply fortiori to the pre-emptive foiling of threats to national security (such as terrorist activities). Arguably, it is precisely this dimension of future-proofing that has been consistently rejected by the CJEU in its body of data retention case law.

[6] See A Juszczak and E Sason, 'Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?' (2021) Eucrim 238-266; M Rojszczak, 'The Uncertain Future of Data Retention Laws in the EU: Is a Legislative Reset Possible?' (2021) Computer Law & Security Review.

[7] S Ranchordás and M van 't Schip, 'Future-Proofing Legislation for the Digital Age' in S Ranchordás and Y Roznai (eds), *Time, Law, and Change: An Interdisciplinary Study* (Hart 2020) 10.

may yet evolve in unexpected new directions. Secondly, as electronic communication itself continue to develop, any fresh retention mandate will have to deal with changes in the very notion of "metadata": what data types it is reasonable (in terms of regulatory burden and resources) or even technologically possible to retain, especially on a "suspicionless" basis. Thirdly, future-proofness is reflected in the valid demands of the citizens of democratic societies that any retention scheme be able to demonstrate (an adequate degree of) effectiveness over time.

In retrospect, the now-infamous Data Retention Directive ("DRD") from 2006 was less future-proof than ticking time-bomb.[8] That is where the analysis begins in II., with a brief overview of CJEU case law up to today on communications data retention, summarising the Court's more recent – and controversial – forays into retention for national security purposes, in order to prepare the ground for a discussion of the data retention debate in Europe from a future-proofing perspective in III.

II. "The lighthouse for privacy rights in Europe"?[9] Past and present CJEU case law on communications data retention

II.1. Retain in haste, repent at leisure: the legacy of Directive 2006/24/EC

From 2006 onward the so-called "Data Retention Directive"[10] (the "DRD") committed Member States to imposing obligations on internet access and telecoms providers to retain the subscriber, traffic and location data of all users without exception (but not the content of their communications) for possible later use by law enforcement in the investigation, detection and prosecution of serious crime.[11]

In the years following its entry into force, domestic implementations of the DRD met with resistance especially from civil society and service providers in multiple Member States, drawing challenges before several national (constitutional) courts,[12] before in 2014 the Court of Justice of the European Union (CJEU) famously annulled the Directive

[8] For Markou, writing in 2012, "(t)he Directive has placed a bomb in the privacy of European citizens and has allowed the Member States alone to take measures to prevent it from exploding"; C Markou, 'The Cyprus and Other EU Court Rulings on Data Retention: The Directive as a Privacy Bomb' (2021) Computer Law & Security Review 471.

[9] ECtHR *Case of Big Brother Watch and Others v The United Kingdom* App. nos. 58170/13, 62322/14 and 24960/15 [13 September 2018], Partly Concurring and Partly Dissenting Opinion of Judge Pinto de Albuquerque, para. 59.

[10] Directive (EC) 2006/24 of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[11] "Serious crime" as defined by each Member State in its national law; art. 1 DRD.

[12] See national constitutional Court judgments involving data retention in twelve Member States, M Zubik, J Podkowik and R Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer Nature Switzerland 2021).

in its landmark judgment in *Digital Rights Ireland* on the grounds that it was incompatible with arts 7, 8 and 52(1) of the Charter.

Although that legislation, adopted to harmonise a data retention obligation across the Union, was declared invalid *ab initio*,[13] in the wake of the *Digital Rights Ireland* judgment there remained the question of the Charter-compliance of national data retention regimes – most of which had been adopted in implementation of the DRD, but some of which predated it. National regimes could still seek to rely on an exception to the protections (including an effective prohibition on retaining traffic and location data) set out in the ePrivacy Directive, then as now a key regulatory instrument for electronic communications service (ECS)[14] providers in the EU. Art. 15(1) of that Directive explicitly foresees the adoption of legislative measures providing for the retention of data for a limited period justified on grounds including the prevention, investigation, detection and prosecution of criminal offences – provided that such a restriction respect Charter rights as interpreted by the CJEU.[15]

Following *Digital Rights Ireland*, references for a preliminary ruling in relation to data retention laws in two Member States, Sweden and the UK, reached the Court in 2016. In its judgment in *Tele2 Sverige and Watson* ('*Tele2*'), the Court essentially confirmed its stance in *Digital Rights Ireland*: notwithstanding the room for manoeuvre in art. 15(1) of the ePrivacy Directive, general and indiscriminate retention of traffic and location data is incompatible with arts 7, 8, 11 and art. 52(1) of the Charter.

It is worth underlining that this is so, according to the Court in *Tele2*, even where a hypothetical national law should meet every other condition laid out by the CJEU pertaining to proportionality of retention scope and strength of safeguards against the misuse of retained data (or other irregularities, *e.g.* loss of data).[16] In other words, for the CJEU in *Tele2* no level of substantive trammelling or procedural stringency could render lawful any retention regime which is "general and indiscriminate" (*i.e.* applying to all users, "blanket") of traffic and location data for the fight against even serious crime: that would constitute a *per se* irredeemably disproportionate interference with the aforementioned Charter rights.[17]

[13] *I.e.*, from 3rd May 2006, meaning the April 2014 judgment's retroactive effects stretched back fully eight years.

[14] Since *Digital Rights Ireland* was decided, the ambit of "Electronic Communications Service" (ECS) under EU law has been expanded to include, notably, some "over-the-top" (OTT) service providers such as instant messaging and "voice-over-IP" (VoIP) services; the interplay between technological change, the regulatory framework and metadata retention for the purposes of combatting crime is discussed in section III.1 and III.2 below.

[15] Art. 15(1) of Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('ePrivacy Directive').

[16] *Ibid.*

[17] Retention of *content* data (for instance, recordings of telephone conversations or the message "inside" emails) the CJEU importantly underlined, would constitute the most serious violation of all – by violating the very essence of the relevant Charter rights. For a critical analysis of this aspect of the Court's reasoning, see M

By contrast, continued the Court, "targeted" retention may be permissible "provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary"[18] and "meet[s] objective criteria, that establish a connection between the data to be retained and the objective pursued".[19] What such a "targeted" retention scheme might look like, also in light of subsequent elaborations from the Court and recent developments in a handful of Member States, will be discussed at III.1. below.

Legislative and judicial responses at national level to *Tele2* have varied significantly over the years since 2016 and remain in a state of flux. Some Member States have replaced or amended – in some cases, more than once – their national laws with the stated aim of ensuring compliance with the CJEU jurisprudence. In other Member States, national implementations of the DRD were subsequently struck down and have not yet been replaced. In yet others, domestic laws implementing the annulled DRD are still in place.[20]

At EU level meanwhile, ever since *Tele2* the prospect of fresh legislation has waited in the wings – without any draft proposal surfacing – as the Court has gradually refined as well as expanded its case law on communications data retention.

References from Spain[21] and Estonia[22] have seen the Court confirm the stance taken on retention *per se* in *Digital Rights Ireland* and *Tele2* whilst providing important clarifications on the matter of access to retained data. If those two cases might be labelled "access

Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) German Law Journal 864-883, esp. 871-874.

[18] *Tele2* cit. para. 108.

[19] *Ibid*. para. 110.

[20] For a snapshot of the most recent developments, see Report of the European Union Agency for Fundamental Rights (FRA), 'Fundamental Rights Report' (2022) 180-181. The FRA put together an overview in 2017 after *Tele2* of steps taken by Member States to bring national laws into line with that ruling. See also Privacy International, 'National Data Retention Laws since the CJEU's Tele-2/Watson Judgment' (September 2017), finding that 40% of the 21 Member States surveyed still had the pre-*Digital Rights Ireland* regime transposing the DRD in place. In 2020, a report commissioned by the European Commission observed "While a handful of Member States have repealed national transposing data retention laws (chiefly due to decisions of their respective Constitutional Courts) most Member States still apply the regime transposing the DRD. A few countries have set up new legal regimes to comply with the CJEU case-law" (page 25). However, no comprehensive overview was provided; the study aimed to collect information on the legal frameworks and practices for retention of and access to non-content data at national level, but only covered ten Member States. See European Commission, 'Study on the Retention of Electronic Communications Non-content Data for Law Enforcement Purposes – Final report' (Milieu Consulting 2020).

[21] In *Ministerio Fiscal* (2018) the Court validated access to retained *subscriber* data – a category of data deemed to entail a less-than-serious interference with arts 7 and 8 of the Charter – in cases of less-than-serious crime, whilst confirming the *Tele2* jurisprudence; case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788.

[22] In *HK Prokuratuur* (2021), wherein the Court added that the requirement of independent (judicial or administrative) authorisation of access to traffic and location data cannot be met by a public prosecutor's office whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings; case C-746/18 *H. K. Prokuratuur* ECLI:EU:C:2021:152.

cases",[23] the remaining recent decisions of the Court can be sorted into two categories. Into the first category falls a series of cases mainly concerned with the Charter-compatibility of national laws mandating – as had the DRD – blanket data retention for the fight against serious crime (references from courts in Ireland,[24] Germany[25] and France[26]). Into the second category falls a set of cases which concern not only data retention for the purpose of fighting *crime* but also address for the first time the relationship between EU fundamental rights standards and national regimes involving data retention for the purpose of safeguarding *national security* (references from France, Belgium[27] and the UK[28]).

Whilst this *Article* concentrates on the possible regulatory futures of data retention for the purposes of combatting crime, before crossing that bridge it is necessary to lay the groundwork by summarising the most relevant aspects of recent CJEU case law on data retention and Member State responses thereto, beginning in II.2 with the Court's unprecedented engagement with the lawfulness of data retention for national security purposes, before turning in II.3 to its embryonic vision for sufficiently-"targeted" retention for the purpose of crime prevention.

II.2. *La Quadrature du Net* and Privacy International: from crime to national security (and back)

Of all the rulings thus far handed down in a burgeoning body of case law, it is the two rulings issued on the same day in October 2020 in response to references from courts in France and Belgium (in *La Quadrature du Net*) and the UK (in *Privacy International*) that have indisputably deepened the complexity of the CJEU's stance on data retention – whilst also opening new, if familiar, fissures in the tensions between national (constitutional) law and prerogatives and the limits of EU competence.

On a higher level (and as mentioned above) this is due to the Court's engagement for the first time with national security as a purpose of data retention, leading to its ultimate position to the effect that blanket retention of traffic and location data may be exceptionally permissible for national security purposes whereas it remains irredeemably impermissible for the purpose of fighting crime (however serious). Yet on a closer view too, the rich 2020 rulings take the *Tele2* line of jurisprudence in multiple new directions. As far as

[23] The label is admittedly imperfect, in particular in light of the significance of *H. K. Prokuratuur* on the matter of the admissibility as evidence at criminal trial of data which had been unlawfully retained. At the time of writing a further "access case", referred by an Italian court, is pending at the CJEU: case C-178/22 *Procura della Repubblica presso il Tribunale di Bolzano* (hearing on 21 March 2023).

[24] Case C-140/20 *GD v Commissioner of An Garda Síochána and Others* ECLI:EU:C:2022:258.

[25] Joined cases C-793/19 and C-794/19 *SpaceNet and Telekom Deutschland* ECLI:EU:C:2022:702 ('SpaceNet').

[26] Joined cases C-339/20 and C-397/20 *VD and SR* ECLI:EU:C:2022:703.

[27] Joined cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791.

[28] Case C-623/17 *Privacy International* ECLI:EU:C:2020:790.

data *retention* is concerned,[29] they notably reach beyond the core battleground of traffic and location data as data *categories* by embarking on a proportionality analysis involving 'new' data categories (such as "civil identity data") as well as increasingly granular data *types* (such as source IP addresses). Those data categories and data types are systematically ascribed 'intrusiveness' ratings and in turn arranged in cascading fashion according to a "hierarchy of public interest (security) objectives".[30]

Since the judgments in *La Quadrature du Net* and *Privacy International,* that hierarchy stands as follows:

a) The objective of safeguarding national security is more important than…

b) the objectives of combatting serious crime and serious threats to public security, which are more important than…

c) the objectives of combatting non-serious crime and non-serious threats to public security.

The possible contours of Charter-compliant data retention regimes match and correspond to the above objectives as follows:

a) For national security, general and indiscriminate retention of traffic and location data (including all IP addresses) as well as "civil identity data" is permissible subject to conditions.

b) For serious crime and serious threats to public security, retention of traffic and location data must be "targeted", but source IP addresses and "civil identity data" may be retained generally and indiscriminately.

c) For non-serious crime and non-serious threats to public security, "civil identity data" may be retained generally and indiscriminately.[31]

[29] The rulings also go beyond the retention of data by private actors at all to confront bulk collection and transfer as well as automated analysis carried out by private actors on behalf of the security and/or intelligence services. For this reason alone, any labelling of *La Quadrature du Net* and *Privacy International* as "data retention case law" requires a good measure of nuance. In doing so, the CJEU has furthermore engaged in a broader dialogue with the European Court of Human Rights on the contours of permissible mass surveillance in a democratic society. The CJEU decisions in *La Quadrature du Net* and *Privacy International* arrived on 6 October 2020, after the ECtHR's First Section judgment in *Big Brother Watch and Others v UK* cit. but before the appeal was decided by the Grand Chamber (25 May 2021). See further ECtHR *Centrum för Rättvisa v Sweden* App n. 35252/08 [25 May 2021], decided by the Grand Chamber on the same day as the *Big Brother Watch* appeal. This *Article* will not analyse that case law, instead focusing on the targeted retention of traffic and location data for the purpose of combatting serious crime under EU law.

[30] V Mitsilegas and others, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2022) European Law Journal 6-10.

[31] As mentioned above (n. 17), for a), b) and c), content may never be retained. Additionally, the overview provided here covers only pre-emptive data retention, and not expedited preservation of data (widely known as "quick freeze"). For detailed analysis of the judgments, see for instance M Tzanou and S Karyda, '*Privacy International* and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) European Public Law 123-154; M Zalnieriute, 'A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of the European Union' (2022) Modern Law 198-218.

In placing the safeguarding national security at the top of the above pyramid, the Court observed that the objective of safeguarding it "goes beyond [those] of [...] combating crime in general, even serious crime, and of safeguarding public security", and is "therefore capable of justifying measures entailing more serious interferences with fundamental rights".[32] Ultimately, the Court settled on the permissibility of the retention of the traffic and location data of all users of ECS "for a limited period of time, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat [...] to national security which is shown to be genuine and present or foreseeable".[33] Verification that one of those situations exists must be entrusted to a court or an independent administrative body whose decision is binding, and that review must also encompass a check on the observation of further conditions and safeguards: instructions given to private parties to preventively retain the data of all users must be limited in time to what is strictly necessary (renewals are possible but cannot exceed a foreseeable period of time), and personal data must be effectively protected against the risk of abuse.[34]

It has been noted in the literature that the Court offers no specific justifications or arguments in support of its determination that the safeguarding of national security "goes beyond" the fight against even serious crime; nor, indeed, to substantiate the position that it does so to a degree capable of tipping the balance toward the acceptability of blanket data retention for the first purpose but not the second. *Cela va de soi.* The most obvious explanation for this absence is that the CJEU felt compelled, having first drawn data retention for national security purposes into the scope of EU law on the basis of questionable reasoning, to then apply a less-than-stringent proportionality test to retention carried out in such a politically sensitive area.[35] Whatever the motivations, the putatively clean separation of crime from national security in *La Quadrature du Net* and *Privacy International* immediately raised a series of questions, of which three will be tackled here.

The first question concerned the potential risk, noted by Sajfert shortly after the judgments were released,[36] that Member States would seek to generally and indiscriminately retain data for the purpose of safeguarding national security (permissible, exceptionally, according to the CJEU) only to subsequently use the data in the fight against (serious) crime, for example in an investigation into organised crime – thus leading to an outcome which appears to be self-evidently against the spirit of the judgment, if not necessarily against its letter. This loophole approach had even reportedly been included in a planned

[32] *La Quadrature du Net* cit. para. 136.

[33] *Ibid*. para. 137.

[34] *Ibid*. paras 138-139.

[35] For a discussion of the sustainability of the Court's reasoning in *La Quadrature du Net* and *Privacy International*, see further section III.1 below.

[36] J Sajfert, 'Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy' (26 October 2020) European Law Blog www.europeanlawblog.eu.

reform to the Danish data retention law,[37] before a further judgment from the CJEU confirmed that access to retained data "would be contrary to [the] hierarchy of public interest objectives"[38] and thus impermissible.

The second question raised by this aspect of the judgments in *La Quadrature du Net* and *Privacy International*, which also partly explains the difference of view between the Danish government and the CJEU just outlined, is that it can indeed be challenging in law and in practice to fully separate some of the most serious forms of criminality (to take only one example, terrorist acts[39]) from threats to national security.

By extension, the task of investigating, detecting, prosecuting and especially *preventing* the commission of a serious criminal offence may overlap or even entirely coincide with that of foiling a threat to national security. To a greater or lesser extent depending on the jurisdiction, the respective public authorities – on the one hand, law enforcement, and on the other, security and intelligence services – can and do cooperate, for instance by sharing data (including data initially retained by private entities).[40] With this operational reality (at least in some Member States) front of mind, at the hearings in subsequent data retention cases before the CJEU some Member States as well as the European Commission accordingly argued that some *very* serious crimes should be assimilated to national security and thus be deemed capable of justifying blanket retention of traffic and location data. This was rejected by the Advocate General and the Court in *GD*, settling the question within the context of the CJEU case law – although the inclusion of a "halfway house" category of extra-serious crime may yet present an option for future legislation at EU level.[41]

The third question raised by the judgments in *La Quadrature du Net* and *Privacy International* was more fundamental: would (all) Member State governments be willing to accept them?

[37] J Lund, 'The New Danish Data Retention Law: Attempts to Make it Legal Failed After Just Six Days' (15 June 2022) IT-Politisk Forening www.itpol.dk.

[38] *GD* cit. paras 96-100 (cited text from para. 99).

[39] Such as causing extensive destruction to a government or public facility, a transport system, an infrastructure facility etc, as criminalised at EU level pursuant to art. 3(1)(d) of Directive 2017/541/EU of 31 March 2017 on combating terrorism ('the Terrorism Directive') 6-21. Additionally, terrorist groups may also qualify as organised crime groups under the relevant (EU) legislation, at the same time as posing a national security risk; see K Ligeti and M Lassalle, 'The Organised Crime-Terrorism Nexus: How to Address the Issue of ISIS Benefitting from Lucrative Criminal Activities' in M Engelhart and S Roksandić Vidlička (eds), *Dealing with Terrorism: Empirical and Normative Challenges of Fighting the Islamic State* (Max-Planck-Institut, Duncker & Humblot 2019) 73-96.

[40] See in detail I Cameron, 'Metadata Retention and National Security: *Privacy International* and *La Quadrature du Net*' (2021) CMLRev 1433-1472, esp.1462-1463.

[41] According to the AG Sánchez-Bordona: "The difficulties which were made clear when this was debated at the hearing, in relation to defining the offences that could make up that *tertium genus,* confirm that this is not a task to be carried out by a court"; *GD* cit., Opinion of AG Sánchez-Bordona, para. 52. Future regulatory options are discussed at section III.1 below.

It is no secret that the French government has particularly strongly objected to the Court's interpretation of art. 15(1) of the ePrivacy Directive and by extension of that of EU law to cover data retention for national security purposes (not to mention crime prevention, where its view also diverges from that of the Court). Whilst the French government is far from alone in holding such a position, the *Conseil d'État* was the first – and so far remains the only – national court to handle a direct challenge to the primacy of EU law as a consequence of the CJEU rulings in *La Quadrature du Net* and *Privacy International*.

In a nutshell, the French government had taken the extraordinary step of asking the *Conseil d'État* to rule that the CJEU acted *ultra vires* in issuing those rulings. In an April 2021 judgment ('*French Data Network*'), the highest administrative court in France managed to avert a direct clash with the CJEU, dismissing the *ultra vires* head of the government's argument.[42] However, in doing so it also interpreted the scope of "national security" in French law in strikingly broad fashion: for the *Conseil d'État*, the notion (and with it lawful general and indiscriminate retention of traffic and location data) covers not only risks from terrorism but also a host of other threats including serious threats to public peace due to a rise in radical and extremist groups, industrial or scientific espionage, and sabotage.[43] For De Terwangne, in *French Data Network* the *Conseil d'État* gives the impression of respecting EU law without fully applying the lesson it had received in the answers handed down – or as the French judges might see it, handed *across* (or even *up?*) – from the Luxembourg court in response to its questions.[44]

Since that thunderclap from the *Conseil d'État*, sparked by the French government's opposition to what it sees as the CJEU's straying into domestic (state) prerogatives of national security (extending to the definition of that notion), 2022 brought further important judgments from both the *Conseil constitutionnel* and the *Cour de cassation*. On the whole, the former has hemmed more closely to the CJEU's position, in particular supporting the inadmissibility of general and indiscriminate retention of traffic and location data for serious crime,[45] whereas the latter has "taken liberties with the applicable case law of the Grand Chamber [of the CJEU] on both retention of and access to both traffic and location

[42] J Ziller, 'The Conseil d'État refuses to follow the Pied Piper of Karlsruhe' (24 April 2021) Verfassungsblog www.verfassungsblog.de.

[43] *Conseil d'État* Judgment of 21 April 2021 *French Data Network et autres* para. 44. Noting the "particularly acrobatic" reasoning on the relationship between the primacy of EU law and French constitutional norms employed by the *Conseil d'État* in order to arrive at this conclusion, see (in French) É Dubout, 'Le Conseil d'État, gardien de la sécurité' (2021) Revue des droits et libertés fondamentaux; and in detail A Turmo, 'National security as a an exception to EU data protection standards: The judgment of the *Conseil d'État* in *French Data Network and others*' (2022) CMLRev 203-222.

[44] C 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) Revue trimestrielle des droits de l'homme 22.

[45] M Lassalle, 'Conservation et réquisitions des données relatives aux communications électroniques: un débat serein est-il enfin possible?' (2022) Recueil Dalloz 1540.

data",[46] for example by giving its blessing to, as the *Conseil d'État* had *before* the CJEU's judgment in *GD*, the "loophole" use for serious crime of data retained for national security purposes, despite the CJEU clearly disapproving of this practice in *GD*.

On the statute books,[47] in the national apex courts but also in the wider criminal justice system,[48] the data retention controversy in France looks unlikely to fizzle out soon. Of course, that domestic turbulence is not without its ramifications at EU level – most notably, in the ongoing negotiations toward a new ePrivacy Regulation. That instrument is due to repeal and replace the ePrivacy Directive, and thus harbours the opportunity (in the eyes of many interior ministries and governments) to finally dispose of its key provisions, stretched beyond reason by the "activist" judges in Luxembourg. Although progress on the file has been notoriously slow, in what is at the time of writing still the latest available draft of the ePrivacy Regulation – the mandate agreed by the EU Council in February 2021, just months after *La Quadrature du Net* and *Privacy International* – one can clearly see the Member States' desire to remove this particular stone from their shoe. We return to the ePrivacy reform in III.1. below, having first introduced the CJEU's stance on the retention of traffic and location data for the purpose of combatting serious crime in the next sub-section.

II.3. CJEU guidance on "targeted" retention for serious crime

As shown by the overview in II.1., whereas in *La Quadrature du Net* and *Privacy International* the CJEU established that the general and indiscriminate retention of traffic and location data may be exceptionally permissible for the purposes of safeguarding national security, it held firm on its flat opposition to that same practice for the purposes of combatting serious crime. General and indiscriminate retention of traffic and location data for the fight against crime is thus limited to source IP addresses (serious crime only) and "civil identity data" (all crime). Any retention of the more intrusive categories of traffic and location data (once more, limited to serious crime) must be "targeted", as opposed to general and indiscriminate.

The Court's position on "targeted" data retention did not come out of the blue in *La Quadrature du Net* and *Privacy International*; its roots can be traced back to *Tele2*[49] and

[46] X Tracol, 'The joined cases of *Dwyer*, *SpaceNet* 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' (2023) Computer Law & Security Review 12.

[47] For details of recent legislative changes in France, see M Lassalle, 'Conservation et réquisitions des données relatives aux communications électroniques' cit.

[48] For example, Tracol reports that in July 2022 the management board of the National Conference of Prosecutors "violently reacted" to the four judgments of the criminal chamber of the *Cour de cassation*, and "recognised daily infringements of the well-established case law of the Grand Chamber [of the CJEU] on the retention of and access to traffic and location data"; X Tracol, 'The joined cases of *Dwyer*, *SpaceNet* and *VD and SR* before the European Court of Justice' cit. 13.

[49] *Tele2* cit. paras 105-112.

Digital Rights Ireland[50] before it. In the 2020 rulings, the CJEU thus confirmed *Tele2* in stating that Charter-compliance might be secured by "legislation permitting, as a preventive measure, the targeted retention of traffic and location data for the purposes of combating serious crime, preventing serious threats to public security and equally of safeguarding national security, provided that such retention is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary".[51]

In *La Quadrature du Net* and *Privacy International,* the Court developed and clarified its previous two alternative (and non-exhaustive) recommended routes to Charter-compliance: through personal targeting and geographical targeting. The specific guidance offered in each respect is worth citing in full, beginning with personal targeting:

> "As regards the limits to which a data retention measure must be subject, these may, in particular, be determined according to the categories of persons concerned, since art. 14(1) of [the ePrivacy Directive] does not preclude legislation based on objective evidence which makes it possible to target persons whose traffic and location data is likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security.
> In that regard, it must be made clear that the persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective evidence, as posing a threat to public or national security in the Member State concerned".[52]

On geographical targeting, the CJEU advised as follows:

> "The limits on a measure providing for the retention of traffic and location data may also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas".[53]

Taken together, the cited guidance on "targeted" retention raises a whole host of issues ranging from its doubtful added value to law enforcement in terms of crime *prevention* (especially personal targeting), open questions around technical feasibility and readiness (especially geographical targeting), as well as potential risks of discrimination and

[50] *Digital Rights Ireland* cit. para. 59.
[51] *La Quadrature du Net* cit. para. 147.
[52] *Ibid.* para. 148-149.
[53] *Ibid*. para. 150.

stigmatisation (both forms of targeting).[54] In the immediate aftermath of *La Quadrature du Net* and *Privacy International,* several Member States appeared unconvinced of the binding nature of such guidance, ostensibly preferring to treat it as obiter[55] and/or ask (once again, in the case of France) the CJEU to reconsider its position. So it was that in *GD*, *VD and SR* and *SpaceNet* data retention laws in Ireland, France and Germany respectively were defended (once more, in the case of France) by the national governments *not* on the grounds that those laws were already "targeted" in accordance with CJEU case law,[56] but on a variety of other grounds marshalled in an attempt to convince the Court to soften its position – or, failing that, to at least secure a degree of damage limitation.

In *GD*, the Irish defence combined a strong emphasis on the importance to the public interest in combatting serious crime with a reliance on the stated independence of the internal police unit handling access requests.[57] Predictably, this line of argument ran aground, but not without the Court embarking on a panorama of the different investigative measures available to law enforcement which are not the wished-for blanket retention of traffic and location data.[58] In *VD and SR*, meanwhile, the defence of data retention for the purposes of combatting crime as enshrined in French law – in essence, that EU market abuse legislation presupposed the existence of a blanket data retention scheme,[59] thereby clashing with the Court's insistence that such retention must in all cases of serious crime be "targeted" – was also unsurprisingly dismissed by the Grand Chamber.[60]

[54] See further section III.1. below.

[55] On the reluctant judicial response in Italy, see A Malacarne, 'Ancora sulle ricadute della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il "non luogo a provvedere" sulla richiesta del p.m.' (5 May 2021) Sistema Penale www.sistemapenale.it.

[56] On domestic developments in Portugal, see T Violante, 'How the Data Retention Legislation Led to a National Constitutional Crisis in Portugal' (9 June 2022) Verfassungsblog www.verfassungsblog.de.

[57] J Teyssedre, 'Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Síochána*' (2023) CMLRev 569-588.

[58] Another objective of the challenge in *GD* (the "damage limitation" alluded to above) was to seek, as the Belgian government had in *La Quadrature du Net*, to seek to delay the effects of the finding of incompatibility in national law and/or find a way to preserve the admissibility of (illegally) retained data in criminal proceedings (whether appeals, ongoing trials, or future proceedings). The CJEU was unmoved, and stuck closely to its earlier decisions, on the one hand determining that its judgment would produce effects immediately, and on the other placing the ball firmly back in the court of the trial state on the matter of admissibility – although its precise contribution in this area is nuanced. Due to lack of space as well as its focus on future-proofing data retention, this *Article* will not discuss the potential ramifications of the case law in terms of admissibility at trial of retained data.

[59] For instance, under art. 23(2)(g) and (h) of the Market Abuse Regulation competent authorities shall have the power "to require *existing* recordings of telephone conversations, electronic communications or data traffic records held by investment firms, credit institutions or financial institutions", and "to require, in so far as permitted by national law, *existing* data traffic records held by a telecommunications operator [...]" (emphasis added).

[60] "It is clear from the wording of those provisions that they merely provide a framework for that authority's power to 'require' the data available to those operators, which corresponds to access to those

Of the three national regimes at stake in the trio of cases, it is the German law examined in *SpaceNet* that came closest to securing the approval of the Court. Indeed, in many respects the relevant provisions of the German Telecommunications Law (the *Telekommunikationsgesetz*, or *TKG*) would, on an ordinary construction of the term, warrant the label of "targeted": emails entirely exempted, so too the communications of registered confidential services such as religious or social assistance lines, high data security standards, stringent procedural safeguards against abuses at the point of access to retained data, and – perhaps most significant of all – far shorter retention periods than the Court had seen before: 10 weeks for telephony data, source IP, connection and network identifiers IP allocation records, and 4 weeks for location data.

The German Federal Administrative Court had opined in its reference to the CJEU that this combination of an exclusion of certain means of communication or certain categories of data and a limitation of the retention period would "considerably reduce" the risk of establishing a comprehensive profile of the persons concerned.[61] Although in its judgment the CJEU carefully acknowledged the legislator's efforts to circumscribe the national data retention regime in this case, ultimately its response was withering. The proffered exemptions of emails as well as communications of those entities on the social or religious register (1.300 entities, the German government disclosed at the hearing) were seen as negligible.[62] As for short retention periods,

> "the retention of traffic or location data, that are 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 which he or she uses, is in any event serious regardless of the length of the retention period and the quantity or nature of the data retained, when that set of data is liable to allow precise conclusions to be drawn concerning the private life of the person or persons concerned".[63]

The Court reiterated (yet again) that the retention of data and access thereto each constitute separate interferences with Charter rights; as such, even national legislation ensuring full respect for access conditions set down by the Court in its case law "cannot, by its very nature, be capable of either limiting or even remedying the serious interference, which results from the general retention of those data [...]".[64]

The message sent by the CJEU back to the Member States thus appears to be crystal clear: in future, a targeted form of retention of traffic and location data is the only kind

data. Furthermore, the reference made to 'existing' records, such as those 'held' by those operators, suggests that the EU legislature did not intend to lay down rules governing the option open to the national legislature to impose an obligation to retain such records"; para. 70.

[61] *SpaceNet* cit. para. 34.

[62] *Ibid*. paras 80-83. The Court also noted that whereas registered social and religious entities are exempted, the data of users who are subject to a duty of professional secrecy, such as lawyers, doctors and journalists, are retained; *ibid*. para. 82.

[63] *Ibid*. para. 88.

[64] *Ibid*. para. 91.

of retention that might comply with the Charter. As the following section will show, two Member States (Belgium and Luxembourg) have recently taken up the gauntlet and designed "targeted" national data retention schemes. The regulatory choices already made in fashioning those first iterations of targeted data retention at the national level, as well as experiences of implementing such schemes in future, could be of crucial value for any pan-EU "targeted" retention initiative going forward (and to other national systems).

Before reaching that point, however, III. begins by inspecting more closely the ground upon which the CJEU's "targeted" retention requirement sits. In light of both the reasoning used by the CJEU and upcoming regulatory changes, just how durable – in that sense, how future-proof – is the CJEU case law itself? Should the CJEU's position yet shift in future, targeted retention schemes the likes of which are emerging in Belgium and Luxembourg may no longer be required.

III. Future-proof data retention

III.1. How future-proof is the case law? ePrivacy reform and judicial fears of profiling

As it stands, the CJEU's consistent case law points unequivocally to "targeted" retention of traffic and location data; any general and indiscriminate retention of those data categories, no matter how serious the crime, appears destined to trigger incompatibility with the Charter. But just how durable or "future-proof" is that same case law? In this regard, a degree of caution is advised for two main reasons.

The first reason is that, despite the entrenchment of the Court's position in *Tele2* and its elaboration through *La Quadrature du Net* and *Privacy International*, the reasoning upon which the "hierarchy of public interest objectives" is based remains open to scrutiny – and as such, (minor) reversals in future proceedings cannot be discounted. The second reason is that the ePrivacy Directive, the juridical "platform" on which the CJEU's case law rests, is due to be repealed and replaced by an ePrivacy Regulation whose precise impact on data retention regimes remains to be seen. These two reasons will now be unpacked in turn, beginning with the CJEU's reasoning in *La Quadrature du Net* and *Privacy International*.

In order to place data retention for national security purposes at the top of its hierarchy of public interest objectives, the Court first had to establish the applicability of EU law to that mode of retention despite the exclusory language in both art. 4(2) TEU ("[i]n particular, national security remains the sole responsibility of each Member State")[65] and art. 1(3) of the ePrivacy Directive, which reads:

[65] "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*

> "This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law".

Try as they might in written argument and pleadings to marshal the above provisions in an attempt to have data retention for national security purposes declared to fall outside the scope of EU law, the Member States have repeatedly encountered a CJEU which is sticking steadfastly to the *effet utile* reasoning it first used in *Tele2* in order to dismiss analogous arguments in relation to crime. According to that line of reasoning, to exclude national legislative measures requiring the retention of data for the purpose of combatting crime would lead to the limitation clause in art. 15(1) of the ePrivacy Directive[66] being "deprived of any purpose".[67]

The extension in *La Quadrature du Net* and *Privacy International* of that *effet utile* reasoning beyond crime to cover national data retention regimes in place for national security purposes – notwithstanding the emphasis in the aforementioned third sentence of art. 4(2) TEU – has attracted much commentary and some criticism. For Cameron, "[i]t is quite possible to argue that the Member States included both a national security exclusion clause and a national security limitation clause in the Directive in order to be doubly sure that national security was out of bounds for the Court: a "belt and bootstraps" approach."[68]

The Court took a different view, hitching the applicability of the ePrivacy Directive (and necessarily also the Charter) to a test based on personal scope: data processing carried out by the private parties in question (electronic communications service providers) falls within the scope of the Directive, irrespective of its ultimate purpose (in this case, safeguarding national security) whereas the direct implementation by the Member States of measures that derogate from the rule that electronic communications are to be

security remains the sole responsibility of each Member State." (emphasis added); art. 4(2) of the Consolidated version of the Treaty on European Union [2012].

[66] "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in arts 5 and 6, art. 8(1), (2), (3) and (4), and art. 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in art. 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in art. 6(1) and (2) of the Treaty on European Union".

[67] *Tele2* cit. para. 73; confirmed in *Ministerio Fiscal* cit. paras 34-35, and in subsequent case law.

[68] Cameron, 'Metadata Retention and National Security' cit. 1458.

confidential, without imposing processing obligations on providers of ECS, the Directive does not apply – only national law will.[69]

Enter the Member States' positioning on the upcoming ePrivacy Regulation. At the time of writing, the contents of the new law, and in particular whether it will overall maintain, raise or lower the levels of protection afforded by the old ePrivacy 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: art. 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."[70]

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 art. 4(2) TEU.[71] For the European Data Protection Board ("EDPB"), this aspect of the Council mandate "runs against the premise for a consistent EU data protection framework"; 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 *Schrems I* and *Schrems II*. Double standards in this regard risk rendering the CJEU's case law meaningless and cannot be accepted".[72]

These concerns are well-founded, but it is also possible for that case law to itself evolve in different directions – and not only that of further *tightening* the scope of permissible forms of data retention. In this respect, it is worth mentioning Advocate General Szpunar's recent Opinion in *La Quadrature du Net II*, a pending case at the CJEU concerning

[69] Subject to the application of the so-called "Law Enforcement Directive" ("LED"); *Privacy International* cit. para. 48; *La Quadrature du Net* cit. para. 103. The Court recalled that the measures in question must comply with, *inter alia*, national constitutional law and the requirements of the ECHR.

[70] Council, '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) - Mandate for negotiations with EP', 6087/21, 10 February 2021.

[71] *Privacy International* cit. para. 44.

[72] M Tzanou and S Karyda, '*Privacy International* and *Quadrature du Net*' cit. 152-153.

the French "Hadop" copyright law.[73] Although it is a copyright case, both the position taken and the reasoning used by the Advocate General in *La Quadrature du Net II* are of relevance to data retention for the fight against crime more broadly, as will be unpacked in the next two paragraphs.

In his Opinion, the Advocate General has proposed a readjustment of the case law of the CJEU on the interpretation of art. 15(1) of the ePrivacy Directive as regards measures for the retention of IP addresses assigned to the source of a connection. As was seen above, the *La Quadrature du Net* and *Privacy International* jurisprudence limits general and indiscriminate retention of source IP to the purpose of combatting serious crime. In *La Quadrature du Net II,* the Advocate General proposes widening this purpose threshold to include the prevention, investigation, detection and prosecution of "online criminal offences for which the IP address is the *only means* of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified".[74]

The Advocate General's invitation raises a number of discrete questions (what would qualify as an "online criminal offence"? Is this any more straightforward than determining what is "serious crime"?) and it will be intriguing to see how it is handled by the Court in the judgment. For present purposes, it suffices to note the tone of the Opinion, which emphasises the need to avoid "de facto systemic impunity for offences committed exclusively online, not just infringements of intellectual property rights"[75] and, in a hint of the *effet utile* dial swinging back toward effective law enforcement, stresses that limitations of the rights and obligations established in arts 5, 6 and 9 of the ePrivacy Directive may be limited in proportionate fashion in order to pursue a public interest objective, "namely the prevention, investigation, detection and prosecution of criminal offences laid down in legislation *which would otherwise have no effect*".[76]

More fundamentally, however, the true litmus test for the CJEU's stance on data retention for the purposes of combatting crime is likely to be provided by the overall strength of the privacy protections to be included in the upcoming ePrivacy Regulation. art. 7(4) of the 2021 Council mandate text includes a specific provision envisaging data retention measures. The provision itself is minimal; its significance lies in its very inclusion on top of draft art. 11 ("Restrictions"), the equivalent of art. 15 of the ePrivacy Directive – in a subtle but important departure from an earlier Council text adopted under the German Council presidency in the second half of 2020.[77]

Of course, no overhaul of the regulatory framework would alter the applicability of the protections in the Charter. Yet if the moral objection to blanket data retention in the CJEU's standing case law can be distilled down to a strong aversion to widespread

[73] Case C-470/21 *La Quadrature du Net and Others* ECLI:EU:C:2022:838, opinion of AG Szpunar.

[74] *Ibid*. para. 83.

[75] *Ibid*. para. 80.

[76] *Ibid*. para. 85, emphasis added.

[77] See M Tzanou and S Karyda, '*Privacy International* and *Quadrature du Net*' cit. 152, and the sources cited there.

profiling of citizens ("*feelings* of constant surveillance") and fears of a deleterious chilling effect on freedom of expression, its juridical "platform" is to be found in the ePrivacy Directive: to evidence this platform, one need only mention the Court's recurring references to the EU legislature's objectives and priorities at the relevant time in support of its stringent approach to exceptions to the confidentiality and erasure obligations established therein. That time, of course, means the years between the "latest implementation" date for the Data Protection Directive of October 1998,[78] and adoption of the ePrivacy Directive in July 2002 – aeons ago in terms of electronic communications.[79] Two decades on, there can be little doubt that every aspect of the wording and the overall balance struck by the upcoming ePrivacy Regulation will be scrutinised by those aiming to shear the CJEU's data retention case law of its sharpest edges.[80]

III.2. First national "targeted" retention laws: the exception becomes the rule?

For the time being, the Court's position is that any retention of traffic and location data for the purposes of combatting serious crime must be "targeted". In stark contrast to the French response to the *La Quadrature du Net* and *Privacy International* rulings, in Belgium the Constitutional Court struck down the national data retention provisions the very next day. In July 2022, a new law[81] was passed with the stated aim of ensuring compliance with the jurisprudence of the CJEU.

The Belgian e-Privacy Directive implementing law[82] thus limits general and indiscriminate retention (mostly for 12 months after either end of service or end of session) to subscriber data and related usage data,[83] whereas traffic and location data may only be retained, for 12 months[84] for the purposes of combatting serious crime and safeguarding

[78] Art. 32 of Directive 95/46/EU of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive").

[79] For example, *SpaceNet* cit. para. 53, gauging the EU legislature's intent by examining the 2000 proposal and several recitals of the ePrivacy Directive.

[80] L Bertuzzi, 'EPrivacy: EU Legislators Chase Compromise on Processing Electronic Communications Data' (15 November 2022) Euractiv www.euractiv.com.

[81] Belgian Legislator, Law on the collection and preservation of identification data and metadata in the electronic communications sector and the provision of these data to the authorities, 20 July 2022, 61505.

[82] Belgian Legislator, Law on electronic communications, 13 June 2005, 28070.

[83] The latter term (the author's own) also encompasses what might be called "location data", but pertaining only to the *source* of a communication, *e.g.*, the geographical location of a mobile telephone when the service is activated.

[84] Subject to one exception: mobile ECS, date and time of the connection of the terminal equipment to the network in question due to power-on and disconnect from the network in question due to power-off; see art. 162/2, para. 2 10, Belgian e-Privacy implementing law as amended; Law on electronic communications cit.

national security, where a communication starts or ends on equipment located in a designated geographical zone. A zone may be designated in no fewer than five different ways:

a) as a zone which is particularly exposed to national security risks or the commission of serious crime (including ports, railway and metro stations, prisons and customs buildings, and "critical infrastructures");

b) as a zone where there is a serious potential threat to the vital interests of the country or for the essential needs of the population (including buildings listed as economically- or scientifically-important, motorways, public parking areas, the Royal Palace, military domaines, and the Belgian national bank);

c) as a zone where there is a serious potential threat to the interests of international institutions (including the EU, NATO and the UN),

d) as a zone where the "OCAM" threat level is at least at level 3 (on a scale of 1 to 4);[85]

e) or as a zone (concretely, either a judicial province or police zone) where set totals of specified criminal offences[86] have been recorded per 1000 inhabitants on a three-year rolling average (i.e. for 2025, the average over 2022, 2023 and 2024).

The Belgian reform is as complex as it is novel and it would merit its own dedicated analysis, also in comparison with the similar reform announced in early 2023 in Luxembourg.[87] For present purposes, the discussion will be limited to highlighting a few open questions on the nature of the "targeted" retention foreseen in Belgium and its relationship with the CJEU case law.

The first such question is whether it will be possible to credibly portray the geographical calibrations built into the new law as delivering "targeted" retention in compliance with the CJEU's guidance if it should be borne out – as critics have advanced – that their overall

[85] OCAM concentrates on terrorism, extremism and problematic radicalisation. At the time of writing, the national threat level was at 2 ("medium").

[86] The long list in art. 90*ter*, para. 2, of the Belgian *Code d'instruction criminelle*, plus those in para. 4.

[87] The Luxembourg Government, *Sam Tanson presented the draft law on the retention of personal data* gouvernement.lu. The Data Retention Bill proposes to insert a new art. 5bis in the 2005 Law on the Protection of Private Life, establishing the targeted retention of traffic and location data of users who find themselves (even for a moment, if mobile) in a designated geographical zone. In terms of crime, the retention mandate would cover geographical zones with higher risks of preparation and commission of acts of serious criminality, meaning: *a)* Areas (*lieux*) where crimes or *délits* punishable with a maximum term of imprisonment of at least one year are repeatedly committed; *b)* Areas (*lieux*) which, by their "configuration", tend to encourage (*favoriser*) the commission of such offences; *c)* The surroundings and limits of infrastructure where events of national or international stature (*envergure*) are regularly organised; *d)* Areas (*lieux*) which by their nature gather a large number of individuals. Unlike the more detailed, prescriptive Belgian law, more of the inner workings of "targeted retention" is left to secondary legislation in the form of an *Arrêté grand-ducal* (Grand-Ducal Circular). That Circular, a joint product of the *Haut commissariat à la protection nationale* and a specially-constituted consultative commission, would draw the geographical perimeters of each of the above zones, renewable after evaluation every three years. All translations of the Bill (from the French) are the author's own. See further K Ligeti and G Robinson, 'Digital Evidence and the Cooperation of Service Providers in Luxembourg' in V Franssen and S Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (Cambridge University Press forthcoming).

outcome would be to cover the entire Belgian territory and population.[88] Indeed, it has been claimed that due to its enshrinement of low thresholds the new law's crime rates-based retention (the fifth listed above) would on its own amount to blanket coverage of the entire country – before the further four zoning provisions are even taken into account.[89]

On the one hand, the Belgian incorporation of crime rates does respond directly to repeated invitations from the CJEU to focus on average crime rates in order to establish geographical targeting; the Court has gone so far as to defend such an approach as "in principle, not likely [...] to give rise to discrimination, as the criterion drawn from the average rate of serious crime is, in itself, entirely unconnected with any potentially discriminatory factors".[90]

On the other hand, where the outcome is that retention covers the entire territory, this sits as uneasily with the specific warning that the adoption by national legislators of distinctive criteria *other* than a personal or geographic criterion "it being understood that there can be no question of reinstating, by that means, the general and indiscriminate retention of traffic and location data,[91] as it does with the Court's consistently strict aversion to any measures affecting "the entire (European) population". Ultimately, it is submitted here that any regime which results in (near-)total coverage can only be described as "targeted" with a heavy dose of sophistry, since it plainly turns the exception into the rule.

In terms of future-proofness, the Court has been clear that geographical areas "may and, where appropriate, must be amended in accordance with changes in the circumstances that justified their selection, thus making it possible to react to developments in the fight against serious crime".[92] Such facilities are built into the Belgian reform.[93] What the Court has not even implicitly encouraged, however, is legislating for a "targeted" retention scheme with which operators are unable to comply for practical or technical reasons. In such a scenario, the question of fallback options becomes central: in the new Belgian law, notably, where a service provider is unable to localise equipment more precisely than "Belgium", it is to retain either for the entire national territory or, where this is not possible, not

[88] P Breyer, 'Targeted Data Retention: our map explained' (8 June 2022) www.patrick-breyer.de.

[89] The new regime arranges different retention periods on a sliding scale relative to crime rates as follows: 6 months' retention for 3 or 4 recorded offences per 1.000 inhabitants of a relevant geographical zone; 9 months' retention for 5 or 6 recorded offences; and 12 months' retention for 7 or more recorded offences. *In concreto,* according to the calculations put forward by Patrick Breyer MEP, the national average over the past three years sits at 11 offences, with all judicial provinces bar one (Eupen, at 5.5 offences, triggering retention for a period of 9 months) individually meeting the threshold of 7 offences, consequently triggering retention for a period of 12 months across the vast majority of the Belgian territory. *Ibid*.

[90] *SpaceNet* cit. para. 109.

[91] *Ibid*. para. 112.

[92] *Ibid*. para. 111.

[93] Pointedly, the Belgian evaluation report is to specifically include the percentage of the national territory covered by the new traffic and location data retention scheme. A comparable mechanism is also built into the planned Luxembourg reform.

at all. Where a service provider is unable, for technological reasons, to limit data retention to any specified geographical zone, similarly it is required to retain the data necessary to cover the totality of the (presumably, larger) zone, whilst limiting retention outwith the (smaller) specified zone as strictly as its technological means will allow.

These selected features of the Belgian reform make clear that the new generation of data retention legislation coming through in that country (as well as in Luxembourg, if the Bill is adopted) will provide an opportunity to gauge its impact in practice – and potentially also a bellwether for the CJEU's tolerance of such an interpretation of its guidance.[94] Could a similar approach be taken at EU level? In June 2021, the European Commission sought the views of Member State delegations on possible regulatory paths forward including the possibility of harmonising "targeted" retention at the EU level.[95] In response to an access to documents request by *Statewatch*, seven Member States agreed to release their responses to the questionnaire.[96]

Whilst their representativeness cannot be ascertained, delegations' responses on "targeted" retention are telling. In addition to practical difficulty (in some cases, technological impossibility), risks of discrimination or stigmatisation, what emerges is a dim view of the potential added value to law enforcement of targeted retention of traffic and location data in the fight against serious crime. A familiar crime prevention logic is identifiable – blanket retention is, seen through this prism, inevitably preferred over "targeted" retention[97] – but delegations also pointed out specific limitations of the latter. For instance, the German delegation noted:

> "Serious offences are not limited to specific geographical areas, […] and often take place in a private setting. Moreover, the key communications activity frequently takes place somewhere other than the location at which the offense occurs […]. Especially when it comes to organised crime, analysing the communications activities in pro-active phase prior to the deed is of decisive importance for evaluating acts contributing to the principal

[94] In November 2020, a European Parliament resolution called on the European Commission to launch infringement procedures against Member States whose laws implementing the invalidated DRD had not been repealed to bring them into line with the CJEU case law. It remains to be seen whether the European Parliament might issue a comparable call-in relation to the Belgian reform.

[95] See European Council, 'Data Retention – Commission Services Non-Paper' (EC Working Paper 7924-2021) www.statewatch.org.

[96] Unfortunately, another thirteen Member States refused to release the information on the grounds that it would undermine public security; see Statewatch, 'EU: Data Retention Strikes Back? Options for Mass Telecoms Surveillance Under Discussion Again' (1 December 2021) www.statewatch.org.

[97] As the German delegation observed, "both [the DRD], which since has been declared invalid, and the domestic regulations on the generalised retention of data respectively in place derive their rationale from the fact that in order to fight serious crime it is impossible to predict in advance which traffic data will be required for which persons, for which region, and for which period"; German Delegation, Response to EC Working Paper on 'Data Retention – Commission Services Non-Paper' cit. 3.

offence. Concurrently, limiting data retention to a specific geographical area is not particularly useful given the mobility of suspects".[98]

The Netherlands delegation advised *inter alia* that criminals will avoid locations where data is retained, that many forms of (organised) crime cannot be "geographically defined", because location changes are part of the concealment strategy, targeted retention "will most likely not work" for retaining metadata of (potential) perpetrators of crimes like cybercrime or cyber-enabled crime, and for OTT services it is not always possible or legally permissible to determine the location of a user in order to decide if the users' data should be retained.[99] Ultimately, "it is more a theoretical than practical option, but [...] it would be interesting to further (empirically) investigate its operational potential", specifically mentioning the Belgian scheme.

The future-proofness of any EU-level data retention scheme might therefore be boosted by observing the first years of operation of national "targeted" retention schemes such as that already in place in Belgium (and that proposed in Luxembourg) from the perspectives of added value to law enforcement, technical feasibility and impact on fundamental rights. Particularly on the last point, should one ever reach the CJEU it will be interesting to see whether a national data retention scheme such as Belgium's can be accepted as "targeted", in light of both the letter and the spirit of the CJEU's case law, if indeed its ultimate effect is to "target" virtually the entire population of the relevant national territory.

III.3. What we talk about when we talk about data retention: tomorrow's metadata and future necessity

On even a short historical view, the very reason for retention regimes – such as the invalidated DRD and the various impugned national systems discussed in this *Article* – is bound up in successive waves of technological change. From the 1980s onward, in most EU Member States law enforcement actors began to face the possibility of losing access to the "one-stop-shop" for communications data when (monopolistic, state-owned) telecoms providers were replaced by one[100] or multiple competing private firms. In the early

[98] *Ibid*.

[99] Netherlands Delegation, Response to EC Working Paper on 'Data Retention – Commission Services Non-Paper' cit. OTT stands for "over-the-top", denoting services offered "directly" over the internet, in the sense that the provider of that service does not also provide the (infrastructure required to convey) the communication – rather, it uses existing networks such as the Internet and cellular networks. In terms of electronic communications (not media), the most relevant examples are OTT "instant" messaging, which has largely outstripped SMS and MMS, and OTT voice calling, often called Voice over Internet Protocol or "VoIP". The likes of WhatsApp, WeChat, Google Duo, Telegram, and FaceTime offer one or both of these functionalities.

[100] For example in Ireland, where telecommunications services were transferred from central government to a separate State-owned company, Telecom Éireann, in 1983. See TJ McIntyre, 'Data Retention in Ireland: Privacy, policy and proportionality' (2008) Computer Law & Security Review 327-328.

2000s, it was the arrival of flat-rate billing and broadband internet which dovetailed with a strengthening of privacy protections in law – especially in the context of the flexibility offered by a burgeoning internal market – to undermine voluntary retention of unnecessary metadata across the key sectors of fixed and mobile telephony and internet access.

Today, a further migration of communications from ECS to OTT services has already taken place, with the advent of dynamic IP necessitating adaptation of data retention mandates, and an increasing roll-out of end-to-end encryption (E2EE) as standard diminishing the scope for law enforcement access to the content of communications. It should be a simple exercise to include technological review clauses in legislation, whether at EU or national level.[101] But in the not-so-distant future 5G is projected to fully hit its stride in Europe, raising two baskets of issues for data retention mandates that may prove more problematic.[102] The first relates to quantity: far greater quantities of data processed translates into far greater quantities of data to be retained, potentially at greater expense. Thinking optimistically, this could yet translate into greater popular pressure and policy attention on demonstrable usefulness of such schemes (as is discussed separately below). But on a technological level, it is no good providing in law for the retention of data which is inaccessible to the service providers managing it on behalf of their customers. This would appear to be a very real prospect should the roll-out of 5G lead to (greater) use of end-to-end encryption for metadata as well as content.

The changing shape of what is placed into the boxes marked "metadata", "traffic data", "location data" or otherwise is not only a question of legislative or regulatory celerity but also of legitimacy.

Before it was passed in 2005, the usefulness of data retained under the Data Retention Directive for the purposes of combatting serious crime, chiefly terrorism, was largely assumed – controversially, by the Parliament as well as its co-legislators. Before the Directive was annulled by the CJEU, at EU level a lone Commission report tackling this point had been issued, in 2011,[103] and was plagued by a lack of statistics on crime rates and the structural limitations (for many, the fruitlessness) of comparing rules and practices across diverse national criminal justice systems.

Fast forward to today, and the heart of the CJEU's case law is the art. 52(1) proportionality test. In its case law, from *Digital Rights Ireland* to *SpaceNet*, the CJEU has barely

[101] For example, the new Belgian provisions provide for the addition by Royal Decree (a form of secondary legislation) of new data types emerging from technological evolution, for both blanket and targeted retention, subject to confirmation in law within 6 months; see arts 126, paras 1-17 and 126/2, paras 2-10.

[102] European Commission, 'Study on the Retention of Electronic Communications Non-content Data for Law Enforcement Purposes' cit. 112-117.

[103] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks; Communication COM(2011) 225 final from the Commission of 18 April 2011, Evaluation report on the Data Retention Directive, 23-25.

addressed the necessity of pre-emptive data retention – whether of a blanket or targeted nature. Nor is that in its gift, as a court working within the parameters of extant legislation, rights, litigation questions addressed to it, and precedent. Almost 20 years on from the "rush job"[104] that was the DRD, any new data retention scheme will need to meet higher standards. How might *ex post* evaluation of the effectiveness of data retention (transparency, benchmarks, etc) be configured along the lines of CJEU-proof targeted retention? How would *ex post* evaluation be affected if the policy is achieved by "carve-out" (in the ePrivacy Regulation) as opposed to standalone legislation? These questions ought to be much more central to the policy debate moving forward. Future-proofing the fight against serious crime in Europe through pre-emptive data retention mandates (whether those are blanket or targeted) carries a responsibility to demonstrate, over time, a positive impact on the fight against such crime – *sine qua non*.

IV. Conclusion

This *Article* set out to take a future-proofing lens to pre-emptive metadata retention laws, a category of legislative intervention that has struggled in recent times to qualify even as "Court-proof" – in light of Charter rights to privacy, data protection and freedom of expression, as adjudged by the CJEU.

It did so, in the first main part of the analysis (II.), by sketching the complex aftermath of the Data Retention Directive since its annulment in *Digital Rights Ireland* 2014 and providing an up-to-date summary of the expansion and refinement of the leading CJEU case law since that seminal judgment. In the second main part of the analysis (III.), a future-proof perspective was taken to the current "data retention debate" in the EU, with a view to identifying research and policy priorities for the years to come – intended to double as conditions for the adoption of any fresh EU-level (legislative) initiative installing "data retention 2.0" for the purposes of combatting serious crime.

The analysis showed that whilst the CJEU case law establishes strong bulwarks against general and indiscriminate pre-emptive metadata retention, its resilience should not be taken for granted. Whether through creative interpretations in national law of what does and does not qualify as "targeted" retention, or a future softening of the Court's position – which may be brought along depending on the outcome of the ePrivacy Regulation negotiations – a re-introduction of blanket retention of traffic and location data cannot be discounted, especially if such a reform is propelled by the strong political will history teaches us is generated by "high-impact, low-frequency" events such as major terrorist attacks.

Whether retention of metadata is targeted or blanket, the *Article* went on to address two core aspects of the legal mandates imposing that retention: the technological aspect (in particular: what will "metadata" mean in future, will it always be possible to retain it?)

[104] TJ McIntyre, 'Data Retention in Ireland' cit.

and, relatedly, the necessity to credibly ascertain the effectiveness of such schemes for their stated purpose (here, the discussion was limited to serious crime, as opposed to the avoidance of national security risks). If and when a new EU data retention scheme should come to be proposed, legal researchers ought to be prepared to fully engage with the impact assessment process, in order to better complement stakeholders both public and private. In particular, if the Court-approved approach of "targeted retention" is to stay, we will need more substantial work on its potential roll-out at EU level, the transparency of its use, its demonstrable effectiveness, and constant attention to these aspects into the medium- to long-term in view of revision or ultimately repeal.

Although their ramifications are weighty, data retention mandates are narrow, uncomplicated pieces of regulation: in the first place, certain types of data must be retained (and others may not, such as content) by specified private entities for clearly defined periods of time. In that sense, the design of a future-proof data retention scheme rather easily swerves concerns around technological neutrality – or, rather, it largely depends on the future-proofness already built into the underlying regulatory framework to which it constitutes an exception.[105] What such a scheme may not easily swerve, however, is the potential futility brought on by technological change. To take only the most obvious example: if metadata cannot be accessed by electronic communications service providers (if, for instance, it is encrypted end-to-end), it cannot be retained.

To close, it is submitted that therein lies a fruitful and overdue path for future research efforts and policy attention. "Data retention" has most often been viewed in isolation – from other (EU) laws, from other CJEU case law, and even from other investigatory options. This is perhaps understandable, not least in light of the daunting complexity of the case law. Increasingly, however, there is a convergence of policy developments that seem to imply a need for blanket metadata retention and/or indirectly maintain the technological possibility of retention. In other words, the time has come to de-silo the data retention debate in the EU both horizontally and vertically. The new European Production Order, however fast, cannot catch data that has already been deleted. The European Commission's plans for a CSA Regulation[106] may both dampen end-to-end encryption of metadata into the future and imply its retention. Reaching beyond EU law, it will also be important to monitor the impact of the new Second Additional Protocol to the Council of Europe's Cybercrime Convention (the "Budapest Convention"), accelerating the direct disclosure of subscriber information, on the data retention debate at Member State level.

[105] P Ibáñez Colomo, 'Future-Proof Regulation against the Test of Time: The Evolution of European Telecommunications Regulation' (2022) Oxford Journal of Legal Studies 1170-1194.

[106] "CSA" stand for Child Sexual Abuse; see the Proposal COM(2022) 209 final from the Commission of 11 May 2022 for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.