FONDATION ROBERT SCHUMAN

POLICY PAPER

Schuman Paper
n°846
15th September 2026

Jean MAFART

"*Tele 2*", ten years on: embarrassment and controversy over access to digital data

On 21 December 2016, the Court of Justice of the European Union (CJEU) delivered a ruling *Tele 2 Sverige* the scope of which would soon prove to be staggering: it radically altered the conditions under which the judiciary and investigative authorities could use the metadata held by electronic communications operators. A few weeks later a clear-sighted jurist wrote: "*This judgment will be a game-changer for state surveillance in Europe and while it offered an early Christmas gift to privacy campaigners, it is likely to receive a very mixed reaction from EU Member States as such.*" That would be an understatement: far beyond so-called 'state surveillance', the *Tele 2* case law presents Member States with the challenge of better protecting personal data whilst preserving their ability to investigate terrorism, organised crime, espionage and ordinary crime.

Where do we stand ten years on? This question is all the more significant given that the debate is no longer confined to the European Union's 'Justice and Home Affairs' (JHA) sphere: the issue of '*access to data*' is now also being addressed from the perspective of European resilience, as part of a comprehensive approach to security.

WHAT EXACTLY DOES THIS INVOLVE?

Electronic communications – whether by telephone or via the internet – generate an enormous volume of metadata; this connection, traffic and location data has become an essential 'raw material' for intelligence and criminal investigation services. As far as twenty-five years ago, the electronic communications of Richard Reid – the British man who attempted to detonate his 'booby-trapped shoe' on a Paris-Miami flight in December 2001 – revealed his links to terrorist networks associated with al-Qaeda. The use of metadata is all the more crucial given that the widespread adoption of encryption technologies now hinders access to the content itself: all investigators know, for example, that 'telephone tapping' is no longer what it used to be.

To ensure that data is usable, most Member States required electronic communications providers to retain their customers' data for a certain period so that, if necessary, it could be made available to investigative authorities, either within the administrative framework of intelligence gathering or as part of a criminal investigation. This is therefore nothing to do with 'surveillance', as the data remains with the operators, who are simply required to retain it for a certain period with a view to its possible disclosure to the authorities – it is, then, nothing like the methods denounced in his time by Edward Snowden. It is this framework, however, that the CJEU is now calling into question.

The *Tele 2* ruling did not appear out of the blue: in 2014, the *Digital Rights* ruling overturned the Directive of 15 March 2006 – a text adopted in the wake of the terrorist attack in London – which, to a certain extent, harmonised the rules on the retention of connection data across Member

States. The Court observed that "*the data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*". The Court held that such an intrusion into private life required strict safeguards, which the 2006 Directive did not provide.

But the *Tele 2* ruling goes much further: the Court states that, "*while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight*". This type of retention applies, as a matter of fact, "*even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences*." The ruling therefore suggests that data should be collected selectively, on the basis of '*objective criteria*', so as "*to circumscribe, in practice, the extent of that measure and, thus, the public affected*."

Furthermore, the Court confirms that it must exercise particular vigilance when data are processed by the police: the argument – a recurring one in the case-law of both the CJEU and the ECHR – is, in this instance, that "*the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter*".

Yet the selective retention of connection data is an illusion, as the French Council of State explained in terms that were scarcely any more diplomatic: "*Furthermore, targeted data retention […] would be of particularly dubious operational value, since it would not allow […] access to the connection data of a person suspected of an offence who had not previously been identified as likely to commit such an act. Thus, particularly in the case of first-time offenders, but also where perpetrators of criminal offences use mobile phones with pay-as-you-go SIM cards which they use only for a limited period […], the criminal investigation authorities would be unable to access the connection data essential to solving the cases with which they are dealing. Furthermore, it is impossible to define in advance geographical areas where, by their very nature, no serious criminal acts likely to justify the retention of connection data could occur. An obligation to retain connection data limited to certain geographical areas – even assuming it were technically feasible – would thus hinder the work of the investigating authorities in other parts of the national territory where such offences were committed. Finally, no presumption of dangerousness may lawfully be made against individuals on the basis of their place of residence or professional activity to justify the retention of their traffic and location data.*"

Finally, the *Tele 2* case-law did not merely affect the criminal investigation services: it also impaired the use of connection data in the administrative context of intelligence – that is to say, most often in the field of national security, which the European Treaties reserve as "*the sole responsibility of each Member State*" (TEU, Art. 4, para. 2). An operational issue was thus compounded by a question of principle: that of the respective competences of the Union and its Member States; the European intelligence community, whose activities are largely organised outside the Union's legal and institutional framework, viewed the new legal situation as an unjustified obstacle[1].

THE URGENT NEED FOR A RESPONSE AND DEVELOPMENTS AT THE CJEU

Few CJEU rulings have stirred up such emotion within European institutions, as evidenced by the satisfaction expressed by certain NGOs. From 2017 onwards, the issue of 'data retention' became a recurring theme in discussions within the Union's JHA bodies, ranging from expert groups to meetings of interior and justice ministers. In its conclusions dated 23 June 2017, the European Council emphasised

[1] J. Mafart, la Politique européenne de sécurité intérieure, Bruylant, 2015, ch. II.

the need for '*effective access to electronic evidence*' and for ensuring the '*availability of data*'. However, discussions in the Council remained inconclusive for a long time, particularly as the proposed regulation on 'e-privacy', or 'privacy and electronic communications', which could have resolved part of the problem, could not be finalised during the legislative term that ended in 2024 (the Commission finally withdrew it last year).

Pending a highly uncertain European solution, the Member States were on edge. One particularly sordid case caused a stir: whilst in 2015 the Irish courts had sentenced the murderer of a vulnerable young woman to life imprisonment, a crime committed to a backdrop of sadomasochistic practices, the individual argued that he would not have been convicted without the now-banned practice of generalised and indiscriminate data retention. Would the CJEU declare the investigation null and void and result in the release of a sadistic murderer? How many other criminal cases across Europe were at risk of 'falling apart', simply because the investigating authorities had relied on data obtained under a general data retention regime? In 2022, the Court resolved the matter by confirming the prohibition of regimes like this whilst reaffirming the principle of procedural autonomy of Member States: it was solely for them to define the rules governing the admissibility of criminal evidence. In other words, the defendant could not validly argue that Irish law was contrary to that of the EU[2] ; fortunately, he remained in prison. Nevertheless, Ireland was forced to revise its legislation as a matter of urgency.

In the years following the *Tele 2* ruling, most Member States chose not to rush to adapt their domestic law; amongst them, a camp of 'hardliners' even emerged, led by France. Both this stance of aggressive defiance and the choice to simply remain inactive rested on something of a gamble: to 'hold out' until the CJEU's position softened, even if this meant imposing – at the very latest possible moment – reasonable restrictions on data retention or processing regimes to preserve the principle of general data retention. In addition to France, this school of thought included Italy, Spain, Denmark and certain Central and Eastern European states, despite historically rooted fears (as in Germany or Austria) regarding anything that might suggest citizen surveillance. In any event, the hope of preserving the status quo as far as possible was not compatible with mere inaction. In 2018, a head of government made an informal approach to President Juncker to dissuade the Commission from publishing 'guidelines' on the application of the *Tele 2* case law: a document such as this might only have served to remind Member States of the CJEU's requirements and undermine those who, more or less openly, had chosen the path of the status quo. On a much more official note, the Robert Schuman Foundation and the Max Planck Institute organised an interesting symposium in April 2019 in Luxembourg – where, by a happy coincidence, the CJEU has its seat – on '*the protection of European citizens in an ultra-connected world*'. The statement by a senior French judge is worth quoting: "*It is to be feared that the Luxembourg Court has not mastered how the services responsible for investigations manage to identify perpetrators of crimes or members of criminal networks, whose perfect mastery of police techniques leads them to "professionalise" the erasure of traditional traces and clues*." As for selective data retention, it was described as a '*pipe dream*'.

Determined to bring about a shift in the CJEU's position, several national courts sought to provide it with an opportunity to do so. In this regard, the *Quadrature du Net* ruling, in response to preliminary rulings sought by several Member States, represents a crucial step. The Court first clarifies the mechanism by which European law applies in the field of national security: essentially, it holds that the obligations imposed on operators regarding the protection of their customers' privacy (the 2002 'e-Privacy' Directive) form a single, indivisible whole and cannot depend on the purpose for which the data is retained. Therefore, national law prevails only in cases '*where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services*'.

As if to offset this encroachment of European law into the sphere of national security, the CJEU subsequently relaxed the *Tele 2* case law: it accepted

[2] *CJEU, 5 April 2022, G.D. c. Commissioner of An Garda Síochána.*

that a Member State may require operators to retain connection data in a general and indiscriminate manner "*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*".

But where does that leave us when it comes to crime? Firstly, the Court deems that "*the importance of the objective of safeguarding national security, […] goes beyond that of the other objectives*". This results in a hierarchy of objectives (national security, followed by 'combating serious crime' and 'preventing serious threats to public safety', then 'combating crime' and 'safeguarding public safety')[3] which corresponds to a hierarchy of investigative measures based on the degree of intrusion into privacy. In other words, the objective of 'combating crime in general, even serious crime' cannot, like national security, justify the blanket retention of data; it will be necessary to make do with an order for 'expedited retention' (or 'quick freeze'), that is to say, to ask operators, for the purposes of an investigation, to safeguard the integrity of the connection data already in their possession.

Another significant ruling, *Prokuratuur*, is the one in which the CJEU specifies the conditions for access to data (and not for the retention thereof) in a judicial context: on the one hand, such access must be restricted to 'serious crime' (a concept which, incidentally, is not defined in European law) and to the '*prevention of serious threats to public security*'; on the other hand, access must be authorised by a court or an independent authority, except for a '*public prosecutor's office which conducts the investigation and, where appropriate, brings the prosecution*'.

THE DISPARITY IN MEMBER STATES' RESPONSES

The *Quadrature du Net* ruling shook things up somewhat: on the one hand, the Court left the door slightly ajar to the widespread and indiscriminate retention of data for national security purposes; on the other hand, it opened a loophole in terms of criminal matters since, in addition to 'expedited retention', it did not explicitly prohibit the use in judicial proceedings of data retained for administrative national security purposes. The *Prokuratuur* ruling also meant that, despite new restrictions, the focus of privacy protection need not be solely on data retention: the conditions for access could also be revised[4]. This therefore paved the way for the adaptation of national legal frameworks on a more realistic and clearer basis. One cannot help noticing, however, the disparity between these national adaptations.

According to a report published in November 2024 by Eurojust, twelve Member States have revised their data retention schemes following the case law of the CJEU; however, this category encompasses a wide range of situations, as it includes both France and Belgium.

In France, the Council of State has chosen to reassert the primacy of the Constitution and reserves the right to set aside the application of a European directive or regulation where, as interpreted by the CJEU, it '*would have the effect of depriving a constitutional principle of effective safeguards*' (in this case, security) "*which would not enjoy equivalent protection under EU law*"[5]. However, whilst refraining from applying this solution to the case in question, it relied on the more flexible interpretation of the case-law of the CJEU to rule that French legislation was compatible with European law, subject to a number of changes which did in fact take place shortly afterwards. The response by the *Quadrature du Net* came fast: the Council of State was accused of "*permanently legitimising mass surveillance*" and even – to top it all – of "*freeing the French intelligence services from the principles of the rule of law*".

Whilst these accusations may be somewhat exaggerated, it is interesting to note that, from the same *Quadrature du Net* ruling issued by the CJEU, the Belgian Constitutional Court draws conclusions that are very different from those of the Council of State: in a ruling handed down the following day, it struck down the Belgian legislation on data retention, holding that the CJEU's ruling requires a 'change of perspective'

[3] *On national security, see J. Mafart, « Sécurité nationale », in H. Moutouh and J. Poirot (dir.), Dictionnaire du renseignement, Perrin, 2018*

[4] *Starting in 2014, the French Council of State had proposed an approach focusing on conditions of access rather than on data retention: recognising that the general and prior collection of connection data was a prerequisite for its use, it recommended that conditions of access be tailored to the specific purpose (terrorism, organised crime, etc.); le Numérique et les droits fondamentaux, annual report, Paris, Conseil d'Etat, 2014.*

[5] *Conseil d'Etat (France), 21 April 2021, Quadrature du Net, § 10. – In its written submissions, the government asked the Council of State to rule ultra vires, that is to say, to set aside the CJEU's judgment on the grounds that it did not respect the division of powers between the Union and its Member States. This was the first time since the Treaty of Rome that such an option had been considered in France (whereas it had already been used in Germany); this illustrates the importance the authorities attached to the matter.*

and that 'the obligation to retain data relating to electronic communications must be the exception, not the rule'. At no point did it contest – as the Council of State explicitly did – the possibility of selective data retention. Consequently, Belgium ultimately revised its legislation much more thoroughly than France: a law dated 20 July 2022 introduced, in particular, data retention obligations limited to certain geographical areas.

It is tempting to wonder how two neighbouring states, with similar legal traditions, can draw such divergent conclusions from the same case law. Judging by the remarks made in 2021 by the President of the CJEU, Belgian Koen Lenaerts, it does, however, appear that both approaches meet the Court's requirements[6]: "*The French Council of State handed down a ruling that was entirely in line with that of the Court of Justice, even though it did voice a few criticisms here and there […]. We have certainly got the message. The Belgian Constitutional Court overturned the entirety of the contested law, without voicing the slightest criticism*." Several other Member States, such as Austria and Denmark, have adopted a selective retention approach based on categories of individuals or geographical areas. However, in addition to the issues of principle and effectiveness already mentioned, this approach poses real problems of technical feasibility and cost for operators. Other Member States tailor retention rules according to the nature of the data: Sweden, for example (where the operator *Tele 2* is established), applies much more restrictive rules to geolocation data than to traffic data or simple IP addresses.

The Eurojust study also reveals that three Member States have retained extensive data retention obligations based on the 2006 Directive (the one invalidated by the *Digital Rights* ruling). Spain and Greece, in particular, had, well before 2016, introduced very strict control over access to data as part of their general data retention regime: a judge is involved in all cases, even when the data is accessed for administrative intelligence purposes. Italy, under pressure from the CJEU, has adopted this model of relatively broad data retention subject to authorisation by a judge (rather than the public prosecutor's office). As for Poland, it is under pressure from both European courts: in 2024, the European Court of Human Rights (ECHR) ruled that Polish legislation constituted a disproportionate infringement of the right to privacy.

Conversely, a few Member States have no mandatory data retention scheme whatsoever, not even a limited one: in Germany, the Netherlands, Slovenia and Romania, the investigating authorities – who are limited to 'expedited retention' – are entirely dependent on data retained by operators for their own technical or commercial purposes. The Romanian Constitutional Court did not wait for the *Tele 2* case: on the basis of the Constitution, rather than EU law, it struck down the national legislation transposing the 2006 European Directive in 2009 and again in 2014, on the grounds of a lack of proportionality – both in terms of the conditions for data retention and the conditions for access. The absence of any data retention obligation has led to real problems, as noted in 2024 by a group of experts: "*As a result, investigations are often a race against time, as investigators need to identify the provider of the data and transmit the request […] before the data is deleted, which is sometimes a matter of days or hours. In some cases, companies do not provide information on the specific data that they process and hold, making it difficult for competent authorities […]*."

Experts ultimately agree on two points: on the one hand, less data is available in Member States, either because the national legal framework is weak or because the courts or the operators themselves rely on European case law to adopt a very restrictive approach to data retention or access; on the other hand, the reduced availability of data at European level and the disparity between national regimes affect cooperation on security matters, particularly in the context of European investigation orders.

OUTLOOK

As the tenth anniversary of *Tele 2* approaches, the idea of European harmonisation continues to attract considerable attention. It has logic on its side: the extreme weakness of certain national measures represents a clear vulnerability for the entire area of

[6] *K. Lenaerts, Hearing before the Committee on European Affairs, Paris, National Assembly, Minutes No. 191, 18 May 2021. President Lenaerts added that the Council of State "had fully implemented our judgment".*

freedom, security and justice, given that terrorism and organised crime ignore internal borders. Several examples, such as those of Ireland, Belgium and Denmark, also demonstrate just how precarious an '*old-style*' national data retention regime can be. But it is also clear that, compared with the directive struck down by the *Digital Rights* ruling, a new text will require greater precision and more specific guidance on the protection of privacy, without compromising the operational capabilities of Member States. Herein lies the problem: certain Member States, such as France and Italy, may legitimately fear that a European text strictly aligned with the *Tele 2* case law could weaken the legal framework they have managed to preserve. Engaged in what one imagines to be delicate preparatory work, the European Commission has not yet set out any clear guidelines. In its internal security strategy of April 2025, moreover, it adopted a very cautious tone, announcing that it would "*prepare an impact assessment in 2025 with a view to updating rules on data retention at EU level, as appropriate*"[7]. In short, the debate over a future directive will undoubtedly be fraught with enormous difficulties.

Several recent developments – not to mention possible future decisions by the CJEU – nevertheless tend to favour a more practical approach to the issue of data. 'Access to data', first and foremost, has become a subject in its own right in European debates. In June 2023, a high-level group (HLG) '*on data access for effective policing*' was set up, comprising representatives from the Member States, the Commission, European agencies and the European Counter-Terrorism Coordinator. The European Union is not the only one thinking about this: within the G7, a working group has been established on the same topic. European work reveals that, whilst the development of digital technologies generates vast amounts of potentially usable data, it also has another, less anticipated effect: "*Paradoxically, while the digital transformation has led to the creation, transmission and storage of an ever greater volume of data, the availability of and access to electronic evidence […] has emerged as the main challenge in order to protect the Union's citizens against the threat posed by terrorism and serious and organised crime. – While this challenge is not new, it continues to grow in significance every day. Law enforcement is literally 'going dark'.*"

This high level group's final report also addresses the issue of encryption: "*Data stored on certain types of modern devices protected by crypto chips or protected by strong encryption algorithms and complex passwords cannot be accessed by LEAs, even using the most powerful decryption platforms. Encryption and other cybersecurity and privacy measures are necessary to protect information systems and communication and personal data, but these measures […] reduce the ability of law enforcement to gather evidence.*" The HLG therefore calls on the Commission "*to draw up and implement a technology roadmap focused on the challenges of encryption, addressing all relevant aspects, including those relating to technology, the market, cybersecurity, fundamental rights, standardisation, law enforcement and research*". More broadly, the aim is to establish a legal and technological framework for 'lawful interception', in cooperation with the industry.

The forty-two proposals, presented to ministers in December 2024, promise several years of intense discussions. In its internal security strategy, the Commission states that it will propose a 'roadmap' to '*ensure lawful and effective access to data*' – thus going well beyond the difficulties arising from the *Tele 2* case law. It should also be noted that the Regulation and the Directive of 12 July 2023 on cross-border access to electronic evidence represent a huge step forward in terms of access to the digital data essential to investigations, particularly where such data is held by multinational internet companies[8].

A second notable trend is worth highlighting: as part of a comprehensive approach to security that the Commission is steadfastly promoting – not without institutional ambitions vis-à-vis the Member States, in a geopolitical context conducive to progress on 'European sovereignty' – the issue of access to data now appears to be a key factor in Europe's resilience in the face of crises. In October 2024, the report by former Finnish President Sauli Niinistö on crisis *preparedness* and *readiness* was published. The issue

[7] *We are still waiting for the so-called 'impact assessment'.*

[8] *Instead of resorting to the highly restrictive mechanisms of international criminal cooperation to obtain data held by internet companies in the United States or elsewhere, judges can now issue orders directly to these companies, which are required to appoint a 'legal representative' within the European Union to receive and process these orders promptly.*

of access to digital data for investigative services is addressed therein: in line with the conclusions of the high-level group, he recommends "*the creation of a robust framework for lawful access to encrypted data to support the fight of Member States' authorities against espionage, sabotage and terrorism, as well as organised crime*." Whilst the 'preparedness strategy' of March 2025 makes no mention of these aspects, the internal security strategy of April 2025 addressed them directly.

Finally, in January 2026, President von der Leyen announced a European security strategy. The initiative has not convinced all observers: some point to the accumulation of strategic documents and call for a truly useful single document[9]. A great deal of mystery still surrounds this document, but it is unlikely to be similar to previous documents of this kind, notably the 2022 *Strategic Compass*: by addressing European security from the broadest possible perspective, it aims to set out a comprehensive framework for ensuring coherence between the various European and national policies, both internal and external. A useful document would therefore address internal security issues: for example, hybrid threats – a phenomenon of geopolitical origin – have become a major aspect of internal security policies. Ten years on from *Tele 2*, and following on from the Niinistö report, it is therefore to be hoped that the issue of data will be given its rightful place in European strategic thinking.

Jean Mafart

Prefect, former Director of European and International Affairs at the Ministry of the Interior, author of "La Politique européenne de sécurité intérieure" (Bruylant, 2025), member of the Scientific Committee of the Robert Schuman Foundation

[9] *V. F. Koesterke, « The EU is talking strategy: make it worthwhile », Institut Egmont, 24 March 2026 ; P. Veron, « A new European security strategy: what for ? », ECDPN, 3 June 2026 ; P. Vimont, « European Security Strategy : in search of a new ambition », Carnegie Europe, 11 June 2026.*

You can read all of our publications on our site:
www.robert-schuman.eu/en

Publishing Director: Pascale JOANNIN
ISSN 2402-614X