INTELLIGENCE AND TERRORISM: WHEN THE INTERNAL SECURITY CODE IS IN THE SIGHTS OF THE EUROPEAN JUDGE

Pierre Berthelet, Sylvie Peyrou

The CREOGN Research Notes

French Gendarmerie Officers Academy Research Centre

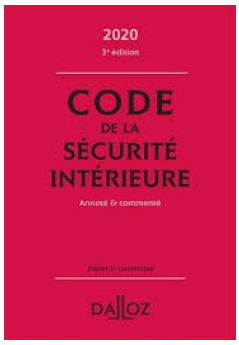
Issue 47 – April 2020

Pierre BERTHELET and Sylvie PEYROU

CREOGN
CENTRE DE RECHERCHE

CVRIA

VERSUS



INTELLIGENCE AND TERRORISM: WHEN THE INTERNAL SECURITY CODE IS IN THE SIGHTS OF THE EUROPEAN JUDGE

In his opinion delivered on 15 January 2020, the Advocate General at the Court of Justice in Luxembourg, Manuel Campos Sánchez-Bordona, opposes the provisions of the Internal Security Code on the collection and retention of data for counter-terrorism purposes. However, he does not question the Code's provisions as such. His analysis focuses first and foremost on the control of proportionality. For some years now, the Court of Justice has been building up a body of case law on the retention of connection data and intelligence tools in the light of European data protection standards. Do these conclusions mark a continuity of the case law or, conversely, the beginning of a shift? One thing is certain, however: they express a very demanding balance between security and freedom.

Title VIII of the Internal Security Code is about to come under the scrutiny of the Court of Justice of the European Union (CJEU). One of its Advocates General, Manuel Campos Sánchez-Bordona, presented on 15 January 2020, conclusions in joined cases (C-511/18 and C-512/18)[1] concerning the collection and retention of data for counter-terrorism purposes. In these conclusions, he opposes legislation "which, in a context marked by serious and persistent threats to national security, and in particular the risk of terrorism, requires operators and providers of electronic communications service providers to retain, in a general and indiscriminate manner, the traffic data and location data of all subscribers" (§ 30 of Case C-511/18), even though the duration of that retention is limited to one year.

These conclusions call into question the measures provided by Articles 851-1 to 6 of the Internal Security Code and Articles L. 34-1 and R. 10-13 of the Post and Electronic Communications Code (as well as Article 6 of Law No. 2004-575 of 21 June 2004 on confidence in the digital economy). This concerns in particular the real-time collection and storage by electronic communications operators of data relating to persons suspected of terrorism (technical data relating to the identification of subscription or connection numbers, the location of mobile phones, numbers called and calling, the duration and date of communications). Several associations, La Quadrature du Net, French Data Network, Igwan.net and the Fédération des fournisseurs d'accès à Internet associatifs had asked the Conseil d'Etat to annul several decrees implementing certain provisions of the Internal Security Code[2].

1 C-511/18 et C-512/18- ECLI:EU:C:2020:6, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs Igwan.net c/ Premier ministre, garde des Sceaux, ministre de la Justice, ministre de l'Intérieur, ministre des Armées.*

2 For more on this visit La Quadrature du Net, « La loi renseignement attaquée devant le Conseil d'État », 10 mai 2016. URL : https://www.laquadrature.net/2016/05/10/loi-renseignement-attaquee-devant-conseil-detat/

These associations consider that the French system for retaining traffic data, location data and connection data violates the provisions of the European Union Charter of Fundamental Rights. More precisely, they consider that the obligations set out in the Internal Security Code constitute, due to their general nature, a disproportionate infringement of the rights to respect for private and family life, to protection of personal data and to freedom of expression. In their view, the inadequate legal framework for data collection and storage practices is contrary to the case law of the Court, first and foremost the Schrems judgment (judgment C-498/16), named after the Austrian citizen who sued Facebook for breach of the right to data protection.
As provided for in the preliminary ruling measures, the Conseil d'Etat, seized by the applicants, addressed the Court, asking it whether the generalized and undifferentiated retention obligation imposed on providers actually constituted a violation of the Charter.
In the background, another European text was questioned, namely Directive 2002/58/EC of 12 July 2002, which concerns the processing of personal data in the electronic communications sector. In its preliminary question, the Conseil d'Etat asked the Court of Justice whether the measures for collecting and using connection data provided for in Article 15(1) of the Directive (and on which French law, in particular the Internal Security Code, is based) constitutes, in the words of the High Administrative Court, "an interference justified by the right to security guaranteed" by the Charter of Fundamental Rights of the Union.

It is necessary to take a step back from this preliminary question because, in his opinion of 15 January 2020, the Advocate General at the CJEU, Campos Sánchez-Bordona, gives his opinion on various cases[3].

In addition to the convergence of legal issues, these three cases will provide an opportunity for the Court to issue a major ruling on data processing in counter-terrorism matters. The conclusions reached are to be watched closely, not only because of the impact that the forthcoming judicial decision will have on the methods of data collection and retention in France, but also in the current construction, by the Court of Luxemburg, of a European law on data protection in anti-terrorist matters.
At the end of the proportionality review, the Advocate General came down against the French provisions, declaring them contrary to EU law (I). The analysis of his conclusions reveals a very demanding balance between security and freedom (II).

I) Provisions of the Internal Security Code contrary to EU law

As a preliminary point, it should be noted that one provision, Article 4(2) of the Treaty of Lisbon, makes national security the exclusive preserve of Member States. However, the Advocate General considers that this article does not preclude the ability of the CJEU to rule on French law relating to national security. This solution is not surprising since it is now settled case law that the Court no longer considers such an article to be an obstacle to case law in anti-terrorism or law enforcement matters (Case C207/16, judgment of 2 October 2018, *Ministerio Fiscal*).
With regard to the case law of the CJEU that may inform the decision it may render in the coming months, one could note that the CJEU considers that the fight against terrorism or crime constitutes a legitimate purpose of such a nature as to ensure the restriction of privacy as well as the retention of data (resp. the judgment of 8 April 2014, *Digital Rights Ireland* and the judgment of 21 December 2016, *Tele2 Sverige and Watson*).

Moreover, since 1964, following the example of the case law of the Conseil d'Etat on public order, the CJEU has rejected indiscriminate and generalised measures, and carefully examined their proportionality. It is in this context that the Advocate General recommends the withdrawal of the provision of the Code of Postal and Electronic Communications obligating operators to retain connection data in an indiscriminate and generalised manner.

3 First cases C-511/18 et C-512/18- ECLI:EU:C:2020:6. Then case C-623/17 – ECLI:EU:C:2020:5, *Privacy International c/ Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*. Finally, case C-520/18 – ECLI:EU:C:2020:7), *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c/ Conseil des ministres*.

It is clear that the legal problem highlighted in the January 2020 conclusions concerns proportionality. However, it must be noted that the Court has shown increased flexibility regarding proportionality in the course of its judgments (see Opinion 1/15 *EU-Canada PNR* delivered on 26 July 2017), followed by the European Court of Human Rights in its *Big Brother Watch* judgment of 13 September 2018[4].

The real issue at stake is whether, as Sylvie Peyrou states, the "gradual shift in case law towards more security at the expense of freedom" will continue or not[5].

The Advocate General seems to want to put a curb on it. It is true that if access to connection data were denied to the investigation and intelligence services, several investigations would be terminated and others could be invalidated, with a significant impact on our national security system. The fact remains that in a state governed by the rule of law, serious flaws vitiate several investigations. In any event, investigations must comply with the legal standard (as highlighted in the Advocate General's distinction between practical effectiveness and legal effectiveness, paragraph 135). The CJEU, aware of the impact of some of its judgments, may limit them in time. That being said, this limitation is refused in view of the seriousness of the infringements (e.g. *Digital Rights Ireland*).

Once the judgment is delivered, the Court's reasoning on the proportionality of the alleged violations will need to be scrutinised. As in the opinion on the EU-Canada PNR agreement, the devil is in the detail.
The European judge may thus invalidate a measure that is deemed insufficient to protect freedoms, for example the procedures for referring cases to the Conseil d'Etat, but at the same time provide the legislator with sufficient legal elements with a view to put in place a protective measures quickly and inexpensively.

In conclusion, a more fundamental question underlies the Court's judgments, that of legal security, at a time when new technologies tend to become central to security and criminal law enforcement policies. However legitimate they may be, developments in data protection law are putting the security structure under pressure, a structure that tends to be based more and more on the use of new technologies, as shown by the recent creation within Europol of the so-called "NAI" knowledge-sharing platform, on "Novel Actionable Information".[6].

II) A very demanding balance between security and freedom

Without recounting all of the Advocate General's arguments, a few points are worth highlighting.
First of all, the Advocate General is clearly aware of the need for national security, particularly in the context of the fight against terrorism. He thus recognises the "right to security" as "inherent in the very existence and survival of democracy" (§ 102 case C-511/18), and affirms the "vital nature for the State" of the fight against terrorism, "an objective of general interest which a State governed by the rule of law cannot renounce" (§ 128 ibid.). But he is equally concerned with respect for the requirements of the rule of law - in terms that deserve to be quoted in extenso - "namely, above all, the submission of power and force to the limits of the law and, in particular, to a legal order whose raison d'être and purpose is the defence of fundamental rights" (§ 130 ibid.). Thus, although it is clear that general and indiscriminate retention of electronic communication metadata by service providers is probably "the most *practical* and *effective* solution (...), the question cannot be asked in terms of *practical effectiveness*, but in terms of *legal effectiveness* and in the context of a state governed by the rule of law" (§ 135 ibid.). If the Advocate General takes care to make long and very pedagogical developments

4 According to Professor Théodore Christakis, « now the Court in Strasbourg takes on a new situation in Europe, namely the growing number of intelligence-related laws having a «blanket surveillance » dimension. In return, the European Court tries to couple this surveillance with guarantees and checks. The issue is no longer about the legality of mass surveillance policies, but rather about «how to apply it » (See original French text in : « Surveillance de masse et CEDH : interview de Théodore Christakis, Victoire à la Pyrrhus », *NetxtImpact.com*, 19 septembre 2018. URL : https://www.nextinpact.com/news/107035-surveillance-masse-et-cedh-interview-theodore-christakis.htm).

5 PEYROU, Sylvie, « Cour de Justice de l'Union européenne, 2 octobre 2018, Ministerio fiscal : la paille et la poutre… », Blog Protection des données et droit de l'Union européenne, 10 octobre 2018. URL : http://www.protection-donnees.eu/2018/10/cour-de-justice-de-lunion-europeenne-2.html).

6 For further detail, cf Pierre Berthelet, « Cybersécurité : l'Europe va se doter d'une nouvelle plate-forme pour mieux lutter contre les criminels », Blog securiteinterieure.fr. URL : https://securiteinterieurefr.blogspot.com/2019/09/cybersecurite-leurope-va-se-doter-dune.html).

in this way, it is obviously in order to guarantee "the impassable barrier of the fundamental rights of citizens" (§ 131), and to avoid that, in the name of efficiency, the State becomes a threat to the citizen.
It is therefore a repeated condemnation of any generalized and indiscriminate retention of communication metadata that the Advocate General calls for in the various cases submitted to his examination, in line with his *Digital Rights Ireland7* or *Tele2 Sverige* jurisprudence[8].

Unaffected by the efforts of the authorities from the Member States to "qualify" his case law in the light of the requirements of the fight against terrorism, the Advocate General once again demonstrates a great deal of pedagogy in his conclusions, delivering a sort of vademecum for the national authorities concerned and in particular for the legislator.
First of all, with regard to access to data, he recalls the importance of prior control by a court or an independent administrative authority[9], a requirement emphasised both in Luxemburg (*Tele2 Sverige* judgment) and in Strasbourg (Court of Human Rights, *Zakharov v. Russia* judgment for example). But he adds a major specification, "except in duly justified cases of urgency" (§ 139). Urgency therefore appears to be a legitimate reason for derogating from the strict material and procedural conditions for access to retained data by the competent authorities. Duly noted.

His reasoning is similar in his conclusions in Case C-520/18 (Ordre des barreaux francophones et germanophones), where he affirms the possibility for national legislation to provide for an obligation to retain data as broadly and generally as necessary, "in truly *exceptional* situations, characterised by an imminent threat or by an extraordinary risk justifying the official determination of the emergency situation in the Member State" (§ 105).
Urgency and exceptional situations therefore open a loophole in the presumed absolute prohibition on the general and indiscriminate retention of the data in question.
The Advocate General also makes a detailed analysis of the provisions of the Internal Security Code which, again in the context of the prevention of terrorism, require the collection in real time of information (traffic data and location data) relating to previously identified persons. Such a technique, which by definition does not imply generalized and indiscriminate storage of data, is thus validated by the Advocate General, provided that the procedures and guarantees in terms of access to data are respected.

Finally, the Advocate General, who is fully aware that targeted data retention - in accordance with the requirements of the case law, for example in the *Tele2 Sverige* judgment - presents a number of practical or legal difficulties, calls on the legislator to devise suitable options that could satisfy the two requirements of any state governed by the rule of law, which are apparently so difficult to reconcile, i.e. combating terrorism and protecting personal data, i.e. security versus freedom. To do this, he suggests using the avenues explored by the Council's working groups (§ 92 aff. Ordre des Barreaux francophones et germanophones). He denies the Luxemburg judge any competence in this regulatory task aimed at specifying, for example, which categories of data may be stored and for how long, this being the responsibility of the legislator of the Union or of the Member States. It is up to the latter to "place the cursor in the right place" (§ 101) in order to ensure the indispensable balance mentioned.
An additional remark by the Advocate General may, however, be considered unfortunate by the commentator: when he admits that giving up information that can be deduced from a greater number of retained data could, in certain cases, make it more difficult to combat potential threats, and when he considers that "this is one price, among others, that the public authorities must pay when they impose on themselves the obligation to safeguard fundamental rights" (§ 102), it is not certain that this point of view will win the support of the Member States and their public opinions...

7 See, for example, our commentary : "La Cour de justice, garante du droit "constitutionnel" à la protection des données à caractère personnel, CJUE 8 april 2014, Digital Rights Ireland, aff. jointes C-293/12, C-594/12, RTDE janvier-mars 2015, p. 117-131.

8 Cf Sylvie Peyrou, « Bis repetita…Member States cannot impose a generalized data retention obligation on electronic communications service providers (Reflections on the CJEU judgment of 21 December 2016, *Tele2 Sverige* AB (C203/15) and Secretary of State for the Home Department (C698/15) », Blog GDR, 22 December 2016. See initial French quote on URL : http://www.gdr-elsj.eu/2016/12/22/droits-fondamentaux/bis-repetita-etats-membres-ne-peuvent-imposer-obligation-generale-de-conservation-de-donnees-aux-fournisseurs-de-services-de-communications-electroniques-reflexions-a-propos-de-l/

9 Solution chosen by France, which entrusted the Commission nationale de contrôle des techniques de renseignements with this monitoring task.

Finally, although it is safe to assume that the Court will follow the Advocate General's conclusions, it is not entirely impossible that it will adopt a more measured position, in line with the shift in its case law that has been anticipated since its Opinion 1/15 or the *Ministerio Fiscal* judgment, validating the generalized retention of communication data but requiring reinforced material and procedural conditions for the collection, access to and retention of data, thus perhaps giving a new colouring to the unavoidable principle of proportionality, obviously respectful of fundamental rights, but more attentive to the needs of the fight against terrorism.

Pierre BERTHELET *has a PhD in Law, specialised in EU Law, and is a researcher with CREOGN*

Sylvie PEYROU *is Maître de conférences HDR (Senior Lecturer with accreditation to supervise research),*
Université de Pau et des Pays de l'Adour, CDRE Bayonne

Translated by SLT Quentin SCHLITTER and the French Gendarmerie Officers Academy Language Department