European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 225-230
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 20

*Connexion Data Retention: the Phoney War Between the French Council of State and the Court of Justice of the European Union**

Thibault Carrère
(Assistant Lecturer and Researcher at University of Le Mans)

French Council of State, Assembly 21 April 2021, n. 393099

French Council of State refuses to operate an ultra vires review on CJEU decisions and EU law. However, it accepts the possibility to maintain a regulatory act contrary to EU law if withdrawing it affect specific constitutional principles. According to the fact that France is facing serious threats towards national security, the generalised and undifferentiated data retention framed by French legislation is compliant with EU law. However, French Prime Minister must provide for a monitoring mechanism to periodically assess the threats to French National Security. Moreover, the intelligence techniques based on traffic and localisation data retention are in whole compliant to EU law, except on the prior review requirement. Therefore, French authorities must provide for an effective prior review by a court or an independent administrative authority.

ABSTRACT This case note analyses the already famous *French Data Network* ruling handed down by the Council of State. Although, the way in which the court considers the relationship between EU law and national law is innovative, this ruling doesn't definitively resolve the compatibility issues between French law and EU law on data retention.

1. *Introduction*

The *French Data Network* judgement handed down by the French Council of State on 21 April 2021[1], is the outcome of a long procedure that has lasted several years[2]. It is an attempt to reconcile the divergent policies of the Court of Justice of the European Union (CJEU) and the French judge with regard to the retention and use of connection data. It is therefore a fundamental judgement regarding both the relationship between national law and European Union (EU) law and the data legal framework insofar as the latter must reconcile the requirements of security and freedom[3].

The *e-privacy* directive of 12 July 2002, gave states significant leeway to collect data for the purpose of safeguarding 'national security (*i.e.*, State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system'[4]. This latitude given

* Article submitted to double-blind peer review.

[1] CE, ass., 21 April 2021, n. 393099, *French Data Network e. a.*

[2] CE, 26 July 2018, n. 393099, *French Data Network*; CJEU, 6 october 2020, C-511/18, C-512/18, C-520/18, *La Quadrature du net e. a.*

[3] It has also given rise to numerous comments in France, see in particular: B. Bertrand and J. Sirinelli, *Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle*, in *Dalloz IP/IT*, 2021,408 ; J. Roux, *La lucidité d'une fermeté ajustée*, in *Recueil Dalloz,* 2021, 1247 ; T. Douville and H. Gaudin, *Un arrêt sous le signe de l'exceptionnel*, in *Recueil Dalloz,* 2021, 1268 ; L. Azoulai and D. Ritleng, *« L'État, c'est moi ». Le Conseil d'État, la sécurité et la conservation des données*, in *Revue Trimestrielle de Droit européen*, 2021, 349 ; F.-X. Bréchot, *De l'art de concilier l'inconciliable. La Constitution, le droit de l'Union et les données de connexion*, in *Revue Trimestrielle de Droit européen*, 2021, 637 ; A. Iliopoulou-Penot, *La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué*, in *La Semaine Juridique édition Générale*, n. 24, 14 June 2021, 1152 ; D. Simon, *Retour des monologues croisés ? À propos de l'arrêt du Conseil d'État dans l'affaire « French Data »*, in *Europe : actualités du droit de l'Union européenne*, n. 6, June 2021, Étude n. 3; A. Bensamoun, *L'arrêt* French Data Network *ou la voie compliquée du dialogue des juges au sujet des données de connexion*, in *La Gazette du Palais*, 29 June 2021, 20 ; M. Bartolucci, *Le Conseil d'État acte la conservation générale et indifférenciée des données de connexion*, in *La Semaine Juridique Administration et Collectivités territoriales*, n. 28, 12 July 2021, 2222.

[4] Article 15 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 *concerning the processing of personal data and the protection*

to States has greatly benefited France, which has put in place permissive legislation on data collection whether for intelligence, counter-terrorism or anti-crime purposes. This permissive legislation has been rather spared by national judges and in particular the Council of State. However, at the European level, the protection of personal data has been pushed by the CJEU and the exception provided in Article 15 of the *e-privacy* directive has been largely reduced by successive decisions of the judges in Luxembourg[5].

This opposition foreshadowed an important conflict between the Council of State and the Court of Justice. At a time of latent conflicts between the Court of Luxembourg and the Court of Karlsruhe[6] and open conflicts between European and Polish judges[7], the solution adopted by the French Council of State seems to be more respectful of the authority of European case law. Nevertheless, this respect comes at the cost of certain ambiguities that do not definitively defuse the contradictions between European and French case law. Consequently, the Council, by taking an original approach to the relationship between European law and national law (I), manages to partially avoid the conflict in the area of data retention (II). As for the use of intelligence techniques, the Council of State finds that French law is in line with European requirements, except for the absence of a prior review (III).

2. *On the relationship between European Union law and the Constitution: an original approach to a classical conflict*

In its decision of 21 April the Council of State noted a possible contradiction between European law rules, as interpreted by the CJEU, and French constitutional principles. In order to resolve this contradiction, it extended its previous solution (A) and rejected the hypothesis of an *ultra vires* review (B) thereby refusing to follow in the footsteps of the German Constitutional Court.

2.1. *The Reversal of the Arcelor Case*

In order to resolve the discrepancies between national law and European law, the French administrative judge made an innovative application of a solution found in the famous *Arcelor* decision[8]. In this 2007 decision, the Council of State, established, on the basis or article 88-1 of the Constitution, the possibility of reviewing the constitutionality of a regulatory act transposing a directive insofar as the constitutional principle in question does not benefits from an equivalent protection under EU law. Thus, the administrative judge before whom a plea arguing the unconstitutionality of a regulatory act transposing a directive is brought, had, in the first place, to seek whether the constitutional principle in question exists in EU law and whether it enjoys equivalent protection. From that point on, the court has an alternative. If there is indeed equivalence of protection, the administrative judge must ensure the constitutional principle by controlling that the regulatory act complies with the equivalent EU provision, if necessary, as interpreted by the Court of Justice. Thus, the judge substitutes the conventionality review for the constitutionality review. However, if there is no provision in European law that provides an equivalent protection to the constitutional principle, the administrative judge can review the constitutionality of the regulatory act and, in necessary, withdraw it from the legal order, even though it was in conformity with EU law.

The *French Data Network* ruling continues this logic by reversing it. First, the judgement extends the solution adopted for administrative acts transposing a directive to all administrative acts simply adapting domestic law to an EU regulation. The solution of the *Arcelor* case is thus extended. Furthermore, and this is the most important point, the Council of State affirms the possibility for the defendant, presumably the minister whose act is challenged before the court, to argue that the absence of equivalent protection of a constitutional principle in EU law must allow the judge to maintain a regulatory act that is contrary to EU law. In the *Arcelor* case the judge accepted to remove from the legal order a regulatory act that was

of privacy in the electronic communications sector.

[5] See, *inter alia:* CJEU, 8 April 2014, C-293/12 *Digital Rights Ireland and Seitlinger e. a.*; CJEU, 21 December 2016, C-203/15, *Tele2 Sverige*.

[6] BVerfG, 5 May 2020, 2 BvR 859/15, 2 BvR 1651/15, 2 BvR 2006/15, 2 BvR 980/16

[7] K 3/21, 7 October 2021.

[8] CE, 8 February 2007, n. 287110, *Société Arcelor Atlantique et Lorrain e. a.*

unconstitutional but in conformity with EU Law. In this *French Data Network* case, the judge accepted to maintain in the legal order a regulatory act that was constitutional but contrary to EU law, since withdrawing it would 'deprive the constitutional requirement cited by the defendant of effective guarantees' (§ 7). Therefore, this solution strongly reaffirms the primacy of the Constitution over EU law, while limiting it to cases where a constitutional principle has no equivalent in EU law.

The Council of State decision must be understood as an extension of its previous case law. At the same time, the Council proposes an original review that departs from the solution requested by the Prime Minister and developed in European constitutional courts.

2.2. *The reject of the ultra vires review*

One of the peculiarities of this case is that the Prime Minister, as a defence to the contested decree, asked the administrative judge to review the preliminary ruling of the Court of Justice with regard to the division of competences set by the European treaties, and, if necessary, to deduce from the violation of that division the lack of binding force of the aforementioned ruling.

In this decision, the French administrative judge refused to activate this so-called *ultra vires* review to regulate the relationship between EU law and national law (§ 8). It preferred to place itself on another ground: that of the existence of specific constitutional principles, *i.e.* those that do not enjoy an equivalent protection in European law. Nevertheless, in an unprecedented way, the Council of State linked this control to a question of competence. Indeed, it considered that the constitutional principles in question did not benefit from an equivalent protection in EU law, insofar as they apply 'To areas that fall exclusively or essentially under the authority of the Member States pursuant to the Union's founding treaties' (§ 10). Thus, European treaties organize the distribution of competences in which national security and preventing the infringements of public order are Member States' competences, and it is indeed that distribution which justifies the absence of equivalent protection in EU law in matter of national security and protection of public order[9]. Consequently, the rejection of *ultra vires* review does not mean, however, the rejection of a national judicial control of the division of competences between the European Union and the French State.

This decision can be read as a defiance towards the primacy of EU law. However, once the basis of its reasoning laid down, the Council of State applied it in a subtle way, avoiding a head-on conflict with the CJEU regarding the retention of connection data.

3. *On data retention: a partially avoided conflict*

In the present case, the new review exercised by the Council of State could have made it possible to maintain the provisions of national law on data retention. Thus, the Council of State could have set aside the preliminary ruling of the CJEU and give priority to security requirements that have constitutional value (A). Nevertheless, the Council of State partially neutralised this conflict regarding the legal framework of data retention, which raises questions about the durability of its solution (B).

3.1. *The acknowledgment of the conflict*

This decision questioned the generalised and undifferentiated retention of three types of data: traffic and location data, IP addresses and data relating to the civil identity of users. These last two types of data were not really problematic. Indeed, the Council of State quickly noted that the generalised and undifferentiated retention of data relating to the civil identity of users is made possible, by EU law as interpreted by the CJEU, to prevent any type of threat to public security, to investigate, detect and prosecute criminal offences no matter how grave and to safeguard national security (§35-36). As regards to IP addresses, the CJEU is similarly permissive insofar as the retention is a fundamental means of investigation, provided that it is made for a limited period of time and to investigate serious crimes, serious threats to public security or to safeguard national security. The Council of State complied to CJEU's interpretation according to which the use of these means of investigation must be controlled by a judge who will assess *in*

[9] B. Bertrand, J. Sirinelli, *Le Conseil d'État et la conservation des données de connexion : la quadrature du cercle*, 408.

concreto the serious nature of the crime or the threat and the proportionality of the measure (§37-41). Thus, for these two types of data, the administrative judge did not need a constitutional requirement to save the provisions of the Post and Electronic Communications Code and the decree of 25 February 2011.

In fact, the real problem for the administrative judge was the generalised and undifferentiated retention of traffic and location data other than IP addresses. While French law allowed for such retention, the dynamic interpretation of EU law by the CJEU severely limited this possibility. Indeed, the CJEU accepts the generalised and undifferentiated retention of this type of data only for the purpose of safeguarding national security, and rejects it for all crime-fighting purposes, including serious crimes. On the other hand, the CJEU allows for the possibility of targeted data retention, *i. e.* the immediate capture of traffic and location data for a limited period of time, provided that it is done under the supervision of a judge. For this type of data, the Prime Minister put forward several *objectives of constitutional value*: the safeguard of the fundamental interests of the Nation, the prevention of breaches in public order, particularly breaches in the security of property and persons, the tracking of criminal offences' perpetrators and the combat against terrorism. Given the new review mechanism put forward by the Council of State, these constitutional principles could have served as a basis for upholding the regulatory acts that are contrary to EU law.

Nevertheless, the administrative judge gave, at least temporarily, full application to European case law.

3.2. *The neutralisation of the conflict*

First of all, the Council of State noted that there is currently a serious threat to national security in France, both real and foreseeable, based on various indicators: the high risk of terrorist attacks, the malicious acts against French companies, the French military involvement abroad, etc. In this respect, the generalised retention of traffic and location data provided for in Article R. 10-13 of the French Post and Electronic Communications Code is, on the whole, in compliance with EU law, except for the fact that it does not provide for a periodic review of the situation. In short, the Prime Minister must implement a regular monitoring mechanism to establish whether France is subject to a serious threat to national security.

Furthermore, national provisions allowing general and undifferentiated retention of traffic and location data for the purpose of combating crime and preventing threats to public order are contrary to the requirements of the CJEU. However, European judges proposed an intermediate solution by considering targeted and expedited retention of data to be consistent with European law. However, the Council of State noted that there are technical obstacles to targeted retention, *i. e.* retention that is aimed at a specific territory or groups of people. Beyond that, according to the Council, targeted retention presents a high risk of discrimination and would lack operational effectiveness (§53-54). As for the *expedited* retention *i.e.* data retention and preservation for a short period of time, based on a court order, the problem raised by the Council of State is that in order to make it possible and effective, retention must be generalised beforehand. In other words, generalised and undifferentiated retention is a prerequisite to expedited retention; otherwise, it would be impossible to obtain data created before to the court order. From this point of view, the provisions of national law were indeed contrary to EU law. Moreover, the solutions proposed by the CJEU did not fully meet the objectives of constitutional value put forward by the Prime Minister. In the light of its new review, the Council of State could have taken into consideration the full contradiction between national and EU law and upheld the decree in the name of these constitutional objectives. Nevertheless, the Council of State avoided a head-on confrontation with the Court of Justice by repealing the regulatory provisions on the grounds that it was contrary to EU law. It considered that, in any case, the generalised retention of data is possible since, at the date of the decision, France was in a period of serious threat to national security. Therefore, the expedited retention technique can be used to fight crime and to prevent threats to public order insofar the data is, in fact, generally retained. Thus, the repeal of the decree does not deprive any constitutional requirements of effective guarantees (§57-58). The Prime Minister must therefore repeal the decree insofar as it is contrary to EU law and will have six months to adapt these articles to

European requirements.

If this decision is resourceful, it is because, while it enshrined the superiority of constitutional norms over EU norms and the possibility to maintain in the legal order national norms that are contrary to EU law by creating a new kind of control, it used the current situation to avoid having to apply this new possibility. The judge therefore repealed the decree, conformed itself to EU law while retaining the possibility, in the future, to use this control as a weapon against EU law and CJEU's case law. However clever, this solution is not without problems. This solution might not be permanent, because what will happen when France is no longer under serious threat to its national security? Unless one considers that the control of the level of threat is a façade and will always result in the finding of a serious threat to national security, thereby allowing French authorities to practise generalised and undifferentiated data retention, there will have to come a day when this situation changes, and then, what will be the chosen solution? Will the Council of State draw all the consequences of its case law and actually maintain internal provisions that are contrary to EU law, thereby risking an open conflict between Paris and Brussels? The *French Data Network* ruling has therefore bought time, but does not shed much light on the future legal framework of data retention.

Data retention is not a purely intellectual undertaking; it is used for police and intelligence activities. So, the *French Data Network* ruling was also an opportunity for the Council of State to rule on the techniques used by the French intelligence services that are based on the generalised and undifferentiated retention of data.

4. *On intelligence techniques: an apparently limited conflict*

Four intelligence techniques were challenged by the claimants. The first technique guarantees access to stored traffic data by intelligence services (Article L. 851-1 of the Internal Security Code); the second gives them the possibility to collect in real time the data of persons previously identified as posing a terrorist threat (Article L. 851-2); the third allows them to put in place an automated analysis of traffic and location data in order to reveal possible terrorist threats (Article L. 851-3) and the fourth authorises them to collect in real time technical data relating to the location of electronic equipment (Article 851-4).

On the whole, these four techniques were declared compliant with EU law. As a matter of fact, in times of terrorist threats, the CJEU itself leaves considerable latitude to Member States to gather intelligence resources. Nevertheless, these regulatory rules were partially repealed on one specific point: the lack of prior review by a judge or an independent administrative authority (§68-83). This requirement of prior review was enshrined by CJEU case law and reiterated shortly before the commented decision[10]. In France, the existing prior review results from an authorisation delivered by the Prime Minister following the opinion from the *National Commission for the Control of Intelligence techniques* (Commission nationale de contrôle des techniques de renseignement). This commission reviews, among other things, the proportionality of the measure. Although important, this review is not binding. However, if the Prime Minister decides not to follow the opinion of the Commission, the latter may refer the matter to the Council of State, which will exercise its jurisdictional review. In *French Data Network* decision, the Council of State considered, for the first time that these provisions, entrenched by the Decree of 11 January 2015, and the Decree of 16 January 2016, are contrary to EU law and repealed them insofar as they do not provide for a binding prior review of the Prime Minister's decision. Nevertheless, this repeal has a limited scope insofar as, until now, successive prime ministers have always followed the opinion of the National Commission for the Control of Intelligence techniques. Therefore, the retroactive repeal of these provisions is not manifestly excessive. Pending the adoption of new provisions to bring national law into line with EU law, the Prime Minister will not be able to take a decision on the use of intelligence techniques after a contrary opinion from the Commission (§96-98).

*

French legislator and administrative authorities have already taken into account this decision and have adapted national norms to European requirements, without always

[10] CJEU, 21 December 2016, C-203/15 and C 598/15, *Tele2 Sverige AV v. Post-ochtelestyrelsen*and *Secretary of State for the Home Department v. Tom Watson*; CJEU, 2 March 2021, C-746/18, *H. K. v. Prokuratuur*

going along with the administrative judge's recommendations. Thus, the new anti-terrorism act of 30 July 2021, does not make the Commission's opinions directly binding. It provides for immediate referral to the Council of State, which will have to rule within 24 hours, when an authorisation from the Prime Minister is given after an unfavourable opinion from the National Commission for the Control of Intelligence techniques. Therefore, the Prime Minister's decision may not be executed before the ruling of the Council of State, except in cases of extreme urgency[11]. In the same vein, the recent decree of 20 October 2021, repeals the illegal provision of the Post and Electronic Communications Code and those of the 2011 decree[12].

In conclusion, the *French Data Network* judgement will undoubtedly be a landmark in the history of relations between national and EU law. With regard to data law, however, the Council of State managed to comply with EU law by repealing the problematic provisions, while retaining, in the current circumstances, the essential elements of national law, namely the generalised and undifferentiated retention of traffic and location data, as well as the intelligence techniques on which it is based.

[11] Article 18 of Legislative Act n. 2021-998 of 30 July 2021, *relative à la prevention d'actes de terrorisme et au renseignement.*

[12] Decree n. 2021-1362, 20 October 2021, *relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.*