NOTE DU CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

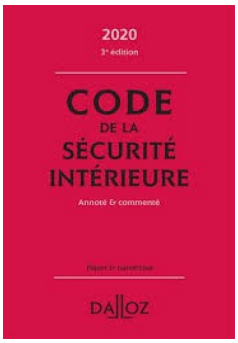
Numéro 47 – Avril 2020

Pierre BERTHELET et Sylvie PEYROU

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

CVRIA

VERSUS



RENSEIGNEMENT ET TERRORISME : QUAND LE CODE DE LA SÉCURITÉ INTÉRIEURE SE TROUVE DANS LE VISEUR DU JUGE EUROPÉEN

Dans des conclusions rendues le 15 janvier 2020, l'Avocat général près la Cour de justice de Luxembourg, Manuel Campos Sánchez-Bordona, s'oppose aux dispositions du Code de la sécurité intérieure relatives au recueil et la conservation des données à des fins de lutte antiterroriste. Toutefois, il ne remet pas en cause en tant que tel le dispositif prévu par le Code. Son analyse porte avant tout sur le contrôle de proportionnalité. Depuis quelques années, la Cour de justice bâtit une jurisprudence en matière de conservation des données de connexion et des outils du renseignement, au regard des standards européens de protection des données. Or, ces conclusions marquent-elles une continuité de la jurisprudence ou, inversement, l'amorce d'un infléchissement ? Une chose est néanmoins sûre, elles expriment un équilibre très exigeant entre la sécurité et la liberté.

Le Titre VIII du Code de la sécurité intérieure va être soumis à l'examen attentif de la Cour de justice de l'Union européenne (CJUE). L'un de ses avocats généraux, Manuel Campos Sánchez-Bordona, a présenté, le 15 janvier 2020, des conclusions dans des affaires jointes (C-511/18 et C-512/18)[1] portant sur le recueil et la conservation des données à des fins de lutte antiterroriste. Dans ces conclusions, il s'oppose à une réglementation « qui, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, impose aux opérateurs et aux prestataires de services de communications électroniques de conserver, de manière générale et indifférenciée, les données relatives au trafic et les données de localisation de tous les abonnés » (§ 30 aff. C-511/18), quand bien même la durée de cette conservation serait limitée à un an.

Est mis en cause dans ces conclusions le dispositif prévu par les articles 851-1 à 6 du Code de la sécurité intérieure ainsi que par les articles L. 34-1 et R. 10-13 du Code des postes et des communications électroniques (de même que l'art. 6 de la loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique). Il s'agit notamment du recueil en temps réel et de la conservation par les opérateurs de communications électroniques des données relatives à des personnes suspectées de terrorisme (données techniques relatives à l'identification des numéros d'abonnement ou de connexion, la localisation des téléphones portables, numéros appelés et appelants, la durée et la date des communications).

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*.

Plusieurs associations, La Quadrature du Net, French Data Network, Igwan.net et la Fédération des fournisseurs d'accès à Internet associatifs avaient demandé au Conseil d'État d'annuler plusieurs décrets d'application de certaines dispositions du Code de la sécurité intérieure[2].
Ces associations considèrent que le dispositif français de conservation de données relatives au trafic, de données de localisation et de données de connexion violent les dispositions de la Charte européenne des droits fondamentaux de l'Union européenne. Plus exactement, elles estiment que les obligations prévues par le Code de la sécurité intérieure constituent, du fait de leur caractère général, une atteinte disproportionnée aux droits au respect de la vie privée et familiale, à la protection des données à caractère personnel et à la liberté d'expression. Selon elles, l'encadrement insuffisant par la loi, des pratiques de recueil et de conservation des données, est contraire à une jurisprudence de la Cour, en premier lieu l'arrêt *Schrems* (arrêt C-498/16) du nom du citoyen autrichien ayant attaqué Facebook pour violation du droit à la protection des données.
Comme le prévoit le mécanisme du recours préjudiciel, le Conseil d'État, saisi par les requérants, s'est adressé à la Cour, lui demandant si l'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs, constituait effectivement une violation de la Charte.
En toile de fond, un autre texte européen est questionné, à savoir la directive 2002/58/CE du 12 juillet 2002, qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques. Le Conseil d'État demande à la Cour, dans sa question préjudicielle, si le dispositif de recueil et d'utilisation de ces données de connexion qu'elle prévoit à son l'article 15, paragraphe 1 (et sur laquelle se fonde le droit français, notamment le Code sur la sécurité intérieure) constitue, selon les termes de la Haute juridiction administrative, « une ingérence justifiée par le droit à la sûreté garanti » par la Charte des droits fondamentaux de l'Union.

Il faut prendre du recul sur cette question préjudicielle car, dans des conclusions du 15 janvier 2020, l'Avocat général près la CJUE Campos Sánchez-Bordona se prononce sur différentes affaires[3].

Outre la convergence des questionnements juridiques, ces trois affaires vont être l'occasion pour la Cour de rendre un arrêt majeur sur le traitement des données en matière antiterroriste. Les conclusions rendues sont à surveiller de près, non seulement de par l'impact que la décision judiciaire à venir va avoir sur les modes de collecte et de conservation des données en France, mais aussi dans l'édification actuelle, par la Cour de Luxembourg, d'un droit européen de la protection des données en matière antiterroriste.
À l'issue du contrôle de proportionnalité, l'Avocat général se prononce défavorablement à l'égard des dispositions françaises en les déclarant comme contraires au droit de l'Union (I). L'analyse de ses conclusions révèle un équilibre très exigeant entre la sécurité et la liberté (II).

I) Les dispositions du Code de la sécurité intérieure contraires au droit de l'Union

À titre liminaire, il convient d'indiquer qu'une disposition, l'article 4, paragraphe 2, TUE fait de la sécurité nationale l'apanage exclusif des États membres. Toutefois, l'Avocat général considère que cet article ne s'oppose pas à la capacité de la CJUE de se prononcer sur le droit français relatif à la sécurité nationale. Cette solution n'a rien de surprenant puisqu'il est désormais de jurisprudence constante que la Cour ne considère plus un tel article comme un obstacle à une jurisprudence en matière antiterroriste ou répressive (aff. C207/16, arrêt du 2 octobre 2018, *Ministerio Fiscal*).

2 Voir à ce sujet 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/

3 D'abord les affaires C-511/18 et C-512/18- ECLI:EU:C:2020:6. Ensuite l'affaire 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*. Enfin l'affaire 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.*

Au regard de la jurisprudence de la CJUE pouvant éclairer la décision qu'elle pourrait rendre dans les prochains mois, il est possible de relever que la CJUE estime que la lutte antiterroriste ou contre la criminalité constitue une finalité légitime de nature à assurer la restriction de la vie privée ainsi que la conservation des données (resp. l'arrêt du 8 avril 2014, *Digital Rights Ireland* et l'arrêt du 21 décembre 2016, *Tele2 Sverige et Watson*).

En outre, depuis 1964, à l'instar de la jurisprudence du Conseil d'État français sur l'ordre public, la CJUE rejette les mesures indifférenciées et généralisées et en étudie attentivement la proportionnalité. C'est dans ce cadre que l'Avocat général préconise le retrait de la disposition du Code des postes et des communications électroniques obligeant les opérateurs à conserver de façon indifférenciée et généralisée les données de connexion.

On l'a compris, la problématique juridique mise en évidence dans les conclusions de janvier 2020 porte à cet égard sur la proportionnalité. Or, force est de constater que la Cour s'est montrée plus souple du point de vue de la proportionnalité au fil de ses arrêts (voir l'avis 1/15 *PNR UE-Canada* rendu le 26 juillet 2017), suivie en cela par la Cour européenne des droits de l'Homme dans sa jurisprudence *Big Brother Watch,* arrêt du 13 septembre 2018[4].

Le véritable enjeu qui se pose actuellement est de savoir si, comme l'énonce Sylvie Peyrou, le « glissement progressif de la jurisprudence, vers plus de sécurité au détriment de la liberté » va se poursuivre ou non[5].

L'Avocat général semble vouloir y mettre un frein. Certes, si l'accès aux données de connexion était dénié aux services d'enquêtes et de renseignement, plusieurs enquêtes prendraient fin et d'autres pourraient être entachées de nullité, avec un impact non négligeable sur notre dispositif de sécurité nationale. Reste que dans un État de droit, des vices graves entachent de nullité plusieurs enquêtes. En tout état de cause, les enquêtes doivent respecter la norme juridique (on peut reprendre l'opposition « efficacité pratique - efficacité juridique » donnée par l'Avocat général paragr. 135). La CJUE, consciente des impacts de certains de ses arrêts, peut les limiter dans le temps. Ceci étant dit, cette limitation est refusée au regard de la gravité des atteintes (par exemple *Digital Rights Ireland*).

Une fois l'arrêt rendu, le raisonnement de la Cour sur la proportionnalité des violations alléguées méritera d'être décortiqué finement. Comme dans l'avis sur l'accord PNR UE-Canada, le diable se cache dans les détails.
Le juge européen peut ainsi invalider un dispositif car jugé insuffisant pour la protection des libertés, par exemple les modalités de saisine du Conseil d'État, mais, en parallèle, donner suffisamment d'éléments juridiques au législateur en vue de mettre en place un dispositif protecteur rapidement et à peu de frais.

Pour conclure, une question plus fondamentale est sous-jacente au fil des arrêts de la Cour, celle de la sécurité juridique, à l'heure où les nouvelles technologies tendent à devenir centrales dans les politiques de sécurité et de répression pénale. Aussi légitimes soient-elles, les évolutions du droit de la protection des données mettent en tension l'édifice de sécurité, un édifice qui tend à se fonder toujours davantage sur l'emploi des nouvelles

4 Selon le Professeur Théodore Christakis, « désormais la Cour de Strasbourg endosse une nouvelle situation en Europe, à savoir la multiplication des lois sur le renseignement ayant une dimension « *surveillance de masse* ». En contrepartie, la Cour européenne essaie d'accompagner cette surveillance de garanties et de contrôles. Il ne s'agit donc plus d'une question concernant la légalité des politiques de surveillance de masse, mais plutôt d'une question liée au « comment l'opérer » (« 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).

technologies, en témoigne la création récente au sein d'Europol de la plateforme dite « NAI » de partage des connaissances, sur les « Nouvelles informations exploitables »[6].

II) Un équilibre très exigeant entre sécurité et liberté

Sans retracer toute l'argumentation de l'Avocat général, quelques points méritent d'être soulignés.
L'Avocat général se montre tout d'abord manifestement conscient des nécessités de la sécurité nationale, notamment dans le contexte de lutte contre le terrorisme. Il reconnaît ainsi le « droit à la sécurité » comme « inhérent à l'existence même et à la survie de la démocratie » (§ 102 aff. C-511/18), et affirme le caractère « vital pour l'État » de la lutte contre le terrorisme, « objectif d'intérêt général auquel un État de droit ne saurait renoncer » (§ 128 ibid.). Mais il s'avère tout aussi soucieux du respect des exigences de l'État de droit – en des termes qui méritent d'être cités *in extenso* – « à savoir avant tout la soumission du pouvoir et de la force aux limites du droit et, en particulier, à un ordre juridique dont la défense des droits fondamentaux constitue la raison d'être et la finalité » (§ 130 ibid.). Ainsi, même s'il est manifeste que la conservation générale et indifférenciée des métadonnées de communication électronique par les fournisseurs de service est sans doute « la solution la plus *pratique* et la plus *efficace* (…), la question ne saurait être posée en termes *d'efficacité pratique*, mais en termes d'*efficacité juridique* et dans le contexte d'un État de droit » (§ 135 ibid.). Si l'avocat général prend soin de faire de la sorte de longs développements très pédagogiques, c'est évidemment afin de garantir « la barrière infranchissable des droits fondamentaux des citoyens » (§ 131), et d'éviter, qu'au nom de l'efficacité, l'État ne devienne une menace pour le citoyen.
C'est donc à une condamnation réitérée de toute conservation généralisée et indifférenciée des métadonnées de communication qu'appelle ici l'Avocat général, dans les diverses affaires soumises à son examen, dans le droit fil de sa jurisprudence *Digital Rights Ireland*[7] ou *Tele2 Sverige*[8].

Insensible aux démarches des autorités des États membres en vue de « nuancer » sa jurisprudence face aux exigences de la lutte contre le terrorisme, l'Avocat général fait montre encore une fois d'une grande pédagogie dans ses conclusions, en livrant en quelque sorte un vade-mecum à destination des autorités nationales concernées et en particulier du législateur.
Il rappelle tout d'abord, s'agissant de l'accès aux données, l'importance d'un contrôle préalable par une juridiction ou une autorité administrative indépendante[9], exigence soulignée tant à Luxembourg (arrêt *Tele2 Sverige*) qu'à Strasbourg (Cour EDH, arrêt *Zakharov c/Russie* par exemple). Mais il ajoute, dans une incise majeure, « sauf cas d'urgence dûment justifié » (§ 139). L'urgence paraît donc comme un motif légitime pour déroger aux strictes conditions matérielles et procédurales d'accès des autorités compétentes aux données conservées. Dont acte.

Son raisonnement est analogue dans ses conclusions à l'affaire C-520/18 (Ordre des barreaux francophones et germanophones), où il affirme la possibilité pour la législation nationale de prévoir une obligation de conservation des données aussi étendue et générale que nécessaire, « dans des situations réellement *exceptionnelles*, caractérisées par une menace imminente ou par un risque extraordinaire justifiant la constatation officielle de la situation d'urgence dans l'État membre » (§ 105).

6 Pour une présentation de ce dispositif, voir 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).

7 Voir, par exemple, notre commentaire : « La Cour de justice, garante du droit "constitutionnel" à la protection des données à caractère personnel, CJUE 8 avril 2014, *Digital Rights Ireland*, aff. jointes C-293/12, C-594/12, RTDE janvier-mars 2015, p. 117-131.

8 Voir Sylvie Peyrou, « Bis repetita…Les États membres ne peuvent pas imposer une obligation générale de conservation de données aux fournisseurs de services de communications électroniques (Réflexions à propos de l'arrêt de la CJUE, 21 décembre 2016, Tele2 Sverige AB (C203/15) et Secretary of State for the Home Department (C698/15) », Blog GDR, 22 décembre 2016. 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 retenue par la France qui confie ce contrôle à la Commission nationale de contrôle des techniques de renseignement.

Urgence et situations exceptionnelles ouvrent donc une brèche face à la présumée interdiction absolue de conservation généralisée et indifférenciée des données en cause.
L'Avocat général, encore, analyse finement les dispositions du Code de la sécurité intérieure imposant, toujours dans le cadre de la prévention du terrorisme, le recueil en temps réel d'informations (données relatives au trafic et données de localisation) relatives à des personnes préalablement identifiées. Une telle technique, qui n'implique pas par définition de conservation généralisée et indifférenciée des données, est validée ainsi par l'Avocat général, du moment que les procédures et garanties prévues en matières d'accès aux données soient respectées.

Enfin, l'Avocat général, tout à fait lucide sur le fait qu'une conservation ciblée des données – conforme aux prescriptions de la jurisprudence, par exemple dans l'arrêt *Tele2 Sverige* – présente un certain nombre de difficultés, pratiques ou juridiques, en appelle alors au législateur afin d'imaginer des formules susceptibles de satisfaire aux deux exigences de tout État de droit apparemment si peu conciliables, la lutte contre le terrorisme et la protection des données personnelles, c'est-à-dire la sécurité contre la liberté. Il suggère pour ce faire de s'appuyer notamment sur les pistes explorées par les groupes de travail du Conseil (§ 92 aff. Ordre des Barreaux francophones et germanophones). Il dénie en effet toute compétence au juge de Luxembourg dans cette tâche réglementaire visant à préciser par exemple quelles catégories de données peuvent être conservées et pour combien de temps, cela étant du ressort du législateur de l'Union ou des États membres. C'est à ce dernier qu'il appartient « de placer le curseur au bon endroit » (§ 101) afin d'assurer l'indispensable équilibre évoqué.
Une remarque additionnelle de l'Avocat général pourra toutefois être jugée malheureuse par le commentateur : quand il admet en effet que renoncer à des informations pouvant être déduites d'un plus grand nombre de données conservées pourrait, dans certains cas, rendre plus difficile la lutte contre les menaces potentielles, et qu'il estime que « c'est un prix, parmi d'autres, que les pouvoirs publics doivent payer lorsqu'ils s'imposent à eux-mêmes l'obligation de sauvegarder les droits fondamentaux » (§ 102), il n'est pas sûr que ce point de vue emporte l'adhésion des États membres et de leurs opinions publiques…

Pour finir, si l'on peut parier que le juge suivra les conclusions de son Avocat général, il n'est pas tout à fait exclu non plus qu'il s'en tienne à une position plus mesurée, allant dans le sens d'un infléchissement pressenti de sa jurisprudence depuis son avis 1/15 ou l'arrêt *Ministerio Fiscal*, validant la rétention généralisée des données de communication mais exigeant des conditions matérielles et procédurales renforcées en matière de recueil, d'accès aux données et de conservation de celles-ci, donnant ainsi peut-être une nouvelle coloration à l'incontournable principe de proportionnalité, respectueuse évidemment des droits fondamentaux, mais plus attentive aux nécessités de la lutte contre le terrorisme.

***Pierre BERTHELET** est Docteur en droit, spécialisé en droit de l'UE et chercheur associé auprès du CREOGN*

***Sylvie PEYROU** est Maître de conférences HDR, Université de Pau et des Pays de l'Adour, CDRE Bayonne*