L'illégalité nuancée de la surveillance numérique

De Terwangne, Cecile

Published in:
Revue trimestrielle des droits de l'homme

Publication date:
2022

Document Version
le PDF de l'éditeur

L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de justice de l'Union européenne

PAR

Cécile de TERWANGNE

Professeure à l'Université de Namur

Directrice de recherche au Centre de recherche Information, Droit et Société (CRIDS)

Résumé

La conservation des données de connexion est au cœur des décisions prononcées par le Conseil d'État français et la Cour constitutionnelle belge à la suite de l'arrêt *La Quadrature du Net* de la Cour de justice. La haute juridiction belge suit la décision de la Cour de justice, confirmant l'illégalité de principe de la conservation massive et indifférenciée de ces données. Des exceptions sont admissibles, notamment pour la protection de la sécurité nationale. Le Conseil d'État, quant à lui, s'autorisera plus de marge pour vérifier que l'interprétation de la Cour de justice ne compromet pas les exigences de la Constitution française, au titre desquelles il fait figurer la sécurité.

Abstract

The retention of connection data is at the heart of the decisions of the French Council of State and the Belgian Constitutional Court following the *La Quadrature du Net* judgment of the Court of Justice. The Belgian high court followed the decision of the Court of Justice confirming the illegality in principle of the massive and undifferentiated retention of such data. Exceptions are admissible, notably for the protection of national security. The Council of State, for its part, will allow itself more leeway to check that the Court of Justice's interpretation does not compromise the requirements of the French Constitution. Following the Council of State, the Constitution includes security.

Introduction

À un jour d'intervalle, les 21 et 22 avril 2021, deux hautes juridictions française et belge se sont prononcées sur la très délicate question de la surveillance numérique par le biais des données de communication. Le Conseil d'État français[1] et la Cour constitutionnelle belge[2] tiraient chacun les leçons de l'arrêt rendu par la Cour de justice six mois auparavant en réponse à leurs questions préjudicielles concernant l'obligation de conservation massive de ces données par les fournisseurs de services de communications électroniques à des fins de lutte contre la criminalité et de sauvegarde de la sécurité nationale.

Cette obligation de conservation généralisée et indifférenciée des données de trafic et de localisation provient initialement de la directive européenne 2006/24/CE[3], qui visait à garantir la disponibilité de ces données pour les autorités publiques. Or, cette directive a été invalidée en 2014 par la Cour de justice dans son retentissant arrêt *Digital Rights Ireland*[4] au motif qu'elle ne satisfaisait pas à l'exigence de proportionnalité. Pour la Cour, la directive entraînait une ingérence d'une vaste ampleur et d'une gravité majeure dans les droits fondamentaux à la vie privée et à la protection des données personnelles, sans que des garanties encadrent une telle ingérence, en assurant que celle-ci demeure limitée au strict nécessaire.

Toutefois, dans l'intervalle, les États membres de l'Union européenne avaient intégré dans leur arsenal législatif l'obligation de conservation massive des données de communication dans le but de favoriser le travail des services d'enquête et de renseignement. Dans cette période marquée par les attentats terroristes, l'intérêt de mettre à disposition des autorités publiques cette mine d'informations était vif. Si l'invalidation de la directive fut saluée par les défenseurs des droits et libertés inquiets de la dérive vers l'instauration d'une société de surveillance, elle a par contre suscité la crainte des autorités publiques d'être privées d'un outil d'« une utilité opérationnelle sans équivalent »[5]. Dans cet état d'esprit, les législateurs nationaux n'ont pas tous revu radicalement leur copie

[1] C.E. (fr.) (ass.), arrêt n° 393.099, *French Data Network e.a.*, 21 avril 2021.

[2] Cour const., arrêt n° 57/2021, 22 avril 2021.

[3] Directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, *J.O.U.E.*, n° L 105 du 13 avril 2006, p. 54.

[4] C.J.U.E., Gde Ch., arrêt *Digital Right Ireland*, 8 avril 2014, aff. jtes n° C-293/12 et n° C-594/12, points 69-71.

[5] Selon les mots du Conseil d'État français (C.J.U.E., Gde Ch., arrêt *La Quadrature du Net e.a.*, 6 octobre 2020, aff. jtes n° C-511/18, n° C-512/18 et n° C-520/18, point 64).

après l'invalidation de la directive. Ainsi, tant la Belgique[6] que la France[7] ont maintenu le principe d'une obligation de conservation généralisée et indifférenciée des données de connexion, même si elles ont modulé quelque peu les garanties entourant cette obligation.

Pourtant, la Cour de justice a poursuivi sur sa voie, et répété les principes qu'elle défend, dans son arrêt *Tele2 Sverige* du 21 décembre 2016[8]. Elle y confirme sa condamnation de la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation tout en reconnaissant aux États le droit de prévoir, à titre préventif, une conservation ciblée de ces données pour lutter contre la criminalité grave, à condition qu'une telle conservation soit limitée au strict nécessaire.

Sur le plan national, les législations française et belge ont été attaquées par les organisations de défense des droits humains, devant le Conseil d'État français, d'une part, et la Cour constitutionnelle belge, d'autre part. Cette dernière était en outre saisie par l'Ordre des barreaux francophones et germanophone, qui était préoccupé de la non-prise en compte de l'obligation de secret professionnel dans la moisson de données réalisée auprès des opérateurs de communications électroniques. Les deux juridictions se sont tournées vers la Cour de justice pour vérifier la compatibilité des régimes de conservation massive des données avec le droit de l'Union. Le 6 octobre 2020, la Cour de justice a apporté sa réponse dans un arrêt prononcé en Grande Chambre, joignant les affaires françaises et belge[9]. Le même jour, la Cour se prononçait, également en formation de Grande Chambre, sur une question très proche concernant l'admissibilité d'une réglementation nationale (la réglementation britannique en l'occurrence) permettant à une autorité étatique d'imposer aux fournisseurs de services de communications électroniques la transmission généralisée et indifférenciée des données de trafic et de localisation aux services de sécurité et de renseignement[10]. Dans ses deux arrêts, la Cour réitère ce qu'elle avait affirmé

[6] Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques.

[7] Article R.10-13 du Code des postes et des communications électroniques ; décret n° 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne ; article 6, II, de la loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique.

[8] C.J.U.E., arrêt *Tele2 Sverige AB c. Post-och telestyrelsen et Secretary of State for the Home Department c. Tom Watson e.a.*, 21 décembre 2016, aff. jtes n° C-203/15 et n° C-698/15.

[9] C.J.U.E., Gde Ch., arrêt *La Quadrature du Net e.a., French Data Network e.a. et Ordre des barreaux francophones et germanophone e.a.*, 6 octobre 2020, aff. jtes n° C-511/18, n° C-512/18 et n° C-520/18.

[10] C.J.U.E., Gde Ch., arrêt *Privacy International*, 6 octobre 2020, aff. C-623/17.

précédemment tout en élargissant le champ des exceptions admissibles au principe de confidentialité des données de communication.

Les juridictions française et belge, édifiées par la réponse obtenue de la Cour de justice, ont donc rendu leurs arrêts de manière presque concomitante. Ces arrêts ne sont pas pour autant allés dans le même sens. Les étonnantes divergences que l'on observe entre les positions des deux hautes juridictions illustrent combien l'équilibre est délicat à trouver entre efficacité des services de sécurité et préservation d'une société démocratique qui ne verse pas dans la surveillance généralisée.

Le présent commentaire commence par clarifier ce que recouvre la notion de données de communication ou de connexion, et relève l'intérêt qu'il y a à les conserver au regard des enquêtes à mener et des infractions à élucider, tout en pointant le danger d'ingérence dans les droits et libertés que ces données représentent (I). Il se penche ensuite sur la protection des droits fondamentaux, tantôt comme justification de la surveillance des communications (II), tantôt, plus classiquement, comme limite, même si cette limite a été redessinée par la Cour de justice dans son arrêt *La Quadrature du Net* (III). Enfin, les surprenantes divergences de vues des deux hautes juridictions belge et française en réaction aux réponses obtenues de la Cour de justice sont abordées dans les deux derniers points (IV et V).

I. Les données de communication : définition et intérêt de leur conservation

Les données qui sont au cœur de cette saga jurisprudentielle correspondent à ce qui est appelé « données de communication », « données de connexion »[11] ou « métadonnées »[12]. Cette notion couvre les données de trafic[13] ainsi que les données de localisation[14]. Il s'agit des numéros de téléphone appelés et appelants, de l'heure d'envoi d'un message ou d'un courrier électronique, des adresses IP utilisées pour naviguer sur internet[15]… Ces données indiquent donc qui utilise un téléphone ou navigue sur le Net, quand, comment et avec qui. Elles renseignent également sur la localisation des appareils terminaux (téléphones mobiles ou fixes, ordinateurs).

Selon la Cour, si elles ne portent pas sur le contenu des messages échangés, ces données prises dans leur ensemble, permettent tout de même de tirer des conclusions très précises sur la vie privée des personnes concernées, « telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[16]. Il est clair que, dans la vie connectée d'aujourd'hui, les données de communication ne se limitent plus à dire qui a appelé qui quel jour, ce qui en soi est déjà révélateur du tissu de relations humaines d'un individu. Ces données dévoilent les centres d'intérêt de chaque utilisateur (les sites internet visités, les pages lues…), les déplacements effectués (en compagnie de qui) et les lieux fréquentés (comme les lieux professionnels, magasins, lieux de culte, hôpitaux, etc.). C'est non seulement la confidentialité des communications et des relations sociales qui est en jeu mais également, potentiellement, de l'état de santé, des opinions politiques et des convictions religieuses, ainsi que l'anonymat des déplacements. Comme le dit le rapporteur public dans ses conclusions concernant l'affaire *French Data Network e.a.*, « [l]es données de connexion ne sont ni plus ni moins que le reflet numérique de votre vie quotidienne, le portable en poche et l'ordinateur en bandoulière. De la couche numérique exsudent des aspects parfois anodins, parfois intimes de votre vie privée, de vos déplacements au supermarché du coin à votre fréquentation récurrente d'une église ou d'une mosquée, d'un club libertin ou d'un bar gay, de votre participation assidue à un forum de *geeks* ou d'alcooliques qu'on hésitera ici à qualifier d'anonymes,

[11] B. Lion, « Conservation des données : pour la Quadrature du Net, la France est 'le seul pays à avoir à ce point tordu la décision de la C.J.U.E.' », *Les Numériques*, 26 avril 2021, consultable à l'adresse www.lesnumeriques.com/vie-du-net/conservation-des-donnees-pour-la-quadrature-du-net-la-france-est-le-seul-pays-a-avoir-a-ce-point-tordu-la-decision-de-la-cjue-n163067.html.

[12] E. Daoud, I. Bello et O. Pecriaux, « Données de connexion et sauvegarde de la sécurité nationale : l'exception confirme la règle », obs. sous C.J.U.E., arrêt *Privacy International*, 6 octobre 2020, aff. C-623/17 et arrêt *La Quadrature du Net e.a.*, 6 octobre 2020, aff. jtes n° C-511/18, n° C-512/18 et n° C-520/18, *Dalloz IP/IT*, 2021, p. 46.

[13] Aux termes de l'article 2, b), de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des →

← communications électroniques (directive vie privée et communications électroniques), les données de trafic sont définies comme « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* ».

[14] Aux termes de l'article 2, c), de la directive 2002/58/CE précitée, les données de localisation sont « *toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ».

[15] Bastien Le Querrec, cité par B. Lion, *op. cit.*

[16] *La Quadrature du Net*, préc., point 117.

d'échanges parfaitement banals avec vos amis au colloque singulier avec votre médecin ou une personnalité politique»[17].

Les services nationaux de sécurité et de renseignement, tant français que belges et britanniques, avaient plaidé qu'empêcher de recueillir toutes ces données impacterait très négativement l'efficacité de leur travail et risquerait de les mettre hors course dans un contexte marqué par des menaces graves et persistantes pour la sécurité, tenant en particulier au risque terroriste, à l'espionnage et à la prolifération nucléaire. Selon eux, la capacité d'acquérir et d'utiliser de telles données présente une utilité sans équivalent, et «les ensembles de métadonnées ainsi constitués devraient être aussi complets que possible, afin de pouvoir disposer d'une 'botte de foin' pour trouver 'l'aiguille' qui s'y dissimule»[18]. Pour le Procureur général français François Molins, «[l]'exploitation de ces données [...] permet, dans une certaine mesure, de lire le passé en retraçant les activités auxquelles un individu s'est livré sur le réseau avant même d'être soupçonné d'activités criminelles, mais aussi de lire le présent avec la géolocalisation. Il s'agit donc pour l'État d'une arme très précieuse, notamment dans la lutte contre la menace terroriste contemporaine dont on connaît le caractère massif ou diffus»[19].

Le législateur belge était lui aussi convaincu de l'utilité de la conservation des données de communication. Il affirme dans l'exposé des motifs de la loi attaquée devant la Cour constitutionnelle que l'objectif poursuivi par ce texte est non seulement de lutter contre le terrorisme et la pédopornographie, mais également de pouvoir utiliser les données conservées dans «une grande variété de situations»: disparition inquiétante, trafic de stupéfiants, vente par internet de médicaments contrefaits, incitations à la haine ou à la violence, harcèlement, espionnage, vol d'identité, *hacking*, chantage, etc.[20].

Sans nier l'intérêt majeur que présentent les données de communication pour mener les enquêtes dans le contexte technologique actuel, on ne peut faire abstraction de l'ingérence particulièrement grave que l'utilisation de ces données induit dans les droits fondamentaux des utilisateurs, ce que n'a pas

[17] A. Lallet, conclusions précédant C.E. (fr.) (ass.), arrêt n° 393.099, préc.

[18] *Privacy International*, préc., point 25.

[19] Fr. Molins, «Droit pénal européen et terrorisme: regard français», *in* Ch. Höhn, I. Saavedra et A. Weyembergh (dir.), *La lutte contre le terrorisme: ses acquis et ses défis / The fight against terrorism: achievements and challenges – Liber amicorum Gilles de Kerchove*, Bruylant, Bruxelles, 2021, p. 151.

[20] Projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques, Exposé des motifs, *Doc. parl.*, Chambre, sess. ord. 2015-2016, n° 54-1567/001, p. 6.

manqué de relever la Cour constitutionnelle belge ainsi qu'on le verra dans les développements qui suivent.

II. La justification de la conservation des données au nom de la protection des droits fondamentaux

A. *Un droit à la sûreté/sécurité?*

Le Conseil d'État français avait demandé à la Cour de justice si une obligation de conservation généralisée et indifférenciée ne devait pas être considérée «comme une ingérence justifiée [notamment] par le droit à la sûreté garanti à l'article 6 de la Charte [...], dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 TUE». La Cour constitutionnelle belge avait elle aussi fait référence dans sa première question adressée à la Cour au droit à la sûreté prévu à l'article 6 de la Charte.

La Cour de justice a profité de ces questions pour clarifier que, si l'article 6 de la Charte, tout comme l'article 5 de la Convention européenne des droits de l'homme, consacre le droit de toute personne à la sûreté, ce droit vise à protéger l'individu contre toute privation de liberté arbitraire ou injustifiée commise par une autorité publique[21]. Il ne s'agit donc pas d'obliger les États à adopter des mesures pour protéger les personnes contre des actes criminels mais plutôt d'exiger d'eux de garantir que nul ne soit privé de sa liberté, sauf dans les cas et conditions prévus par la loi[22].

On ne peut en conséquence confondre le droit à la sûreté avec un droit à la sécurité et il ne peut être question de faire découler du droit protégé à l'article 6 de la Charte et à l'article 5 de la Convention européenne des droits de l'homme un droit de conserver toutes les données de communication en vue d'être à même d'intervenir pour assurer la sécurité des individus.

[21] *La Quadrature du Net*, préc., points 123 et 125.

[22] Avocat général M. Campos Sánchez-Bordona, conclusions présentées le 15 janvier 2020, C.J.U.E., *Ordre des barreaux francophones et germanophone e.a.*, aff. C-520/18, point 99. Voy. Cour eur. dr. h., arrêt *Buzadji c. Moldavie*, 5 juillet 2016, § 84.

B. *Obligation positive d'assurer la protection des droits fondamentaux*

La Cour constitutionnelle belge avait par ailleurs demandé à la Cour de justice si l'on ne pouvait pas considérer que la conservation généralisée des données de communication est en fait destinée à « réaliser les obligations positives incombant à l'autorité en vertu des articles 4 et 8 de la Charte, consistant à prévoir un cadre légal qui permette une enquête pénale effective et une répression effective de l'abus sexuel des mineurs et qui permette effectivement d'identifier l'auteur du délit, même lorsqu'il est fait usage de moyens de communications électroniques ».

L'argument original de la Cour constitutionnelle consistait donc à *justifier* la conservation des données de communication au nom de la protection des droits fondamentaux, plutôt que de *limiter* pareille conservation au nom de cette protection.

La Cour de justice, à la suite de l'avocat général[23], va admettre ce raisonnement. Elle affirme que des obligations positives en matière de lutte contre les infractions pénales peuvent résulter de l'article 7 de la Charte, imposant aux pouvoirs publics d'adopter des mesures pour protéger la vie privée et familiale, le domicile ou les communications, ainsi que des articles 3 et 4 garantissant la protection de l'intégrité physique et psychique des personnes et interdisant la torture et les traitements inhumains et dégradants[24]. Toutefois, les mesures que les autorités sont amenées à prendre au nom de ces obligations positives – parmi lesquelles la conservation des données de trafic et de localisation – doivent pleinement respecter le principe de proportionnalité ainsi que les autres droits et libertés[25]. Il ne s'agit pas de justifier systématiquement la conservation généralisée des données de connexion au nom de la protection des droits à l'intégrité physique et à la vie privée. Mais, dans des circonstances exceptionnelles que la Cour clarifiera (voy. ci-dessous III., B. et C.), la protection de l'intégrité physique et de certains aspects du droit à la vie privée peut paradoxalement justifier une ingérence dans ce droit.

[23] Avocat général M. Campos Sánchez-Bordona, conclusions précitées, points 113 à 118.
[24] *La Quadrature du Net*, préc., point 126.
[25] *Ibid.*, point 128.

III. L'interdiction nuancée de la conservation des données au nom de la protection des droits fondamentaux

A. *La règle maintenue de la confidentialité des données de communication*

La Cour de justice n'a pas été insensible aux arguments développés par les services nationaux de sécurité et de renseignement, mais elle le dit sans ambages : si l'obligation de garantir la confidentialité des communications et des données électroniques prévue à l'article 5 de la directive 2002/58/CE[26] n'est pas absolue et si des dérogations sont bien sûr admissibles sur la base de l'article 15 de cette directive, « il ne peut être question que la dérogation à la règle du secret devienne la règle »[27]. Le droit de l'Union européenne s'oppose à ce qu'une législation nationale fasse peser sur les fournisseurs de services de communications électroniques une obligation généralisée et indifférenciée de conservation des données relatives au trafic et des données de localisation.

Pour la Cour, mettre en place une surveillance systématique des données de communication d'une telle portée porte atteinte non seulement au droit à la vie privée et à la protection des données des individus, mais aussi à la liberté d'expression à partir du moment où toutes les traces des activités de diffusion, de recherche et de partage d'informations sur internet sont enregistrées et analysées. C'est tant la liberté de s'exprimer que celle de s'informer sans faire l'objet d'ingérence d'autorités publiques qui est en jeu. La liberté de la presse est également atteinte dès lors que les communications des journalistes tombent dans le champ de la surveillance. Et il en est de même pour le secret professionnel, notamment celui couvrant les échanges entre les avocats et leurs clients. La Cour relève enfin l'effet dissuasif qui peut affecter les lanceurs d'alerte.

Par ailleurs, il est évident que la conservation d'une telle masse de données pouvant révéler, comme dit plus haut, des informations présentant un carac-

[26] Article 5 de la directive 2002/58 précitée : « *1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1* ».
[27] *Privacy International*, préc., point 59, et *La Quadrature du Net*, préc., point 111.

tère sensible comporte des risques d'abus et d'accès illicite[28]. Ainsi que le relève Jan Janssen, «si elle est mal utilisée, cette même richesse d'informations peut avoir des conséquences particulièrement néfastes. Il suffit de penser à un gouvernement autoritaire qui veut supprimer toute forme d'opposition. L'accès aux données de communication électronique permet de cartographier particulièrement facilement le réseau des opposants au régime»[29].

Inébranlable donc dans son rôle de rempart contre les attaques insistantes contre les droits fondamentaux au nom de l'efficacité de l'action policière et des services de renseignement, la Cour refuse que les États mettent en place une surveillance technologique qui deviendrait la règle. Consciente des défis actuels en termes de sécurité, elle va toutefois apporter dans son arrêt, *La Quadrature du Net*, des nuances à l'exigence démocratique de confidentialité, offrant des perspectives d'action aux services d'enquête. Mais elle sera très claire: les limitations à la règle de la confidentialité ne sont admissibles que dans le respect du principe de proportionnalité et des droits fondamentaux garantis par la Charte.

B. *Enjeu de sécurité nationale, conservation des données et recours aux algorithmes*

C'est principalement pour la préservation de la sécurité nationale, question que la Cour de justice n'avait pas encore abordée dans ses précédents arrêts, que les dérogations les plus larges seront acceptées[30].

Au passage, la Cour ne manque pas de clarifier ce qui est couvert par la notion de sécurité nationale. Cette notion est évoquée à l'article 4, § 2, du Traité sur l'Union européenne qui dispose que la sécurité nationale relève de la responsabilité des États membres. Pour la Cour, «[c]ette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier

[28] *La Quadrature du Net*, préc., point 119.

[29] J. Janssen, «Bewaren of *beware*: dataretentie en grondrechten, een moeilijk evenwicht», *R.A.B.G.*, 2021, n° 8, pp. 673-681.

[30] Ce qui fera dire à un commentateur qu'au nom de la sécurité nationale, «Big Brother can watch everybody» (Chr. Maubernard, «Données personnelles et sécurité nationale: Big Brother can watch everybody», *in* «Les juridictions de l'Union européenne et les droits fondamentaux. Chronique de jurisprudence (2020)», *cette Revue*, 2021, pp. 574 et s.).

à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme»[31].

Il convenait aussi de lever le doute soulevé par plusieurs États membres[32] sur l'applicabilité de la directive 2002/58/CE à des réglementations nationales ayant pour finalité la sauvegarde de la sécurité nationale, normalement compétence exclusive des États membres. La Cour considère cependant que, dès lors que les réglementations nationales imposent aux fournisseurs de services de communications électroniques de conserver des données ou encore de transmettre ces données aux autorités nationales de sécurité et de renseignement, c'est-à-dire d'effectuer nécessairement un traitement des données en question, ces réglementations relèvent du champ d'application de la directive. Il n'en est pas de même, par contre, des mesures qu'un État prendrait directement aux fins de la sécurité nationale, sans imposer d'obligations de traitement de données aux fournisseurs de services de communications électroniques.

Dans les situations où des circonstances suffisamment concrètes permettent de considérer qu'un État fait face à une menace grave pour la sécurité nationale, menace qui s'avère réelle et actuelle ou prévisible, la Cour estime qu'un État peut déroger à l'obligation d'assurer la confidentialité des données de communication électroniques. La loi nationale peut permettre aux autorités, dans de telles circonstances, d'imposer une conservation généralisée et indifférenciée de ces données mais pour une durée limitée au strict nécessaire[33]. Cette durée peut être renouvelée en cas de persistance de la menace mais elle ne peut, chaque fois, dépasser un laps de temps prévisible[34] et le renouvellement ne peut présenter un caractère systématique. En outre, des garanties strictes doivent encadrer l'accès et l'utilisation des données afin de les protéger efficacement contre les risques d'abus. La Cour a donc reconnu que l'importance de la préservation de la sécurité nationale dépasse celle de la lutte contre la criminalité en général, même grave, et peut donc justifier une ingérence plus forte dans les droits fondamentaux[35]. Toutefois, la décision de conservation des données doit être contrôlée par une juridiction ou par une autorité administrative indépendante, afin de vérifier l'existence des circonstances justifiant les mesures prises ainsi que le respect des garanties prévues. On regrettera avec Jan-Jaap

[31] *La Quadrature du Net*, préc., point 135.

[32] La France, la République tchèque, l'Estonie, l'Irlande, Chypre, la Hongrie, la Pologne, la Suède et le Royaume-Uni.

[33] *La Quadrature du Net*, préc., point 137.

[34] *Ibid.*, point 138.

[35] *Ibid.*, point 136.

Oerlemans, Mireille Hagens et Sofie Royer[36] que la Cour n'ait pas été plus claire sur ce qu'elle entendait par «une menace grave pour la sécurité nationale». «S'agit-il uniquement d'une menace réelle d'attaque (terroriste), que la C.J.U.E. mentionne à titre d'exemple, ou également d'un incident de cybersécurité qui menace de perturber l'économie ou cette notion est-elle plus large et couvre par exemple la protection de la sécurité nationale contre le contre-espionnage par des agents de renseignement étrangers?»[37]

La Cour de justice a par ailleurs été amenée à se prononcer également sur le recours à des algorithmes pour traiter la masse gigantesque de données accumulées. Elle estime que ces techniques de filtrage des données en fonction de paramètres prédéterminés, qui sont susceptibles notamment de révéler la nature des informations consultées en ligne, réalisent une ingérence particulièrement grave. Cependant, reconnaissant l'utilité avérée de ces analyses automatisées des données dans la lutte contre le terrorisme, elle admet leur mise en œuvre à la seule fin de cette lutte et de la protection de la sécurité nationale et pourvu qu'elle respecte les mêmes conditions que la conservation des données[38]. La Cour ajoute toutefois à ces conditions l'exigence que les modèles et critères préétablis sur lesquels se fondent les analyses automatisées soient «d'une part, spécifiques et fiables, permettant d'aboutir à des résultats identifiant des individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes et, d'autre part, non discriminatoires»[39]. Par ailleurs, les algorithmes utilisés ne peuvent reposer exclusivement sur des données sensibles telles que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'état de santé ou la vie sexuelle d'une personne. D'autres données liées au comportement individuel de la personne ciblée doivent entrer en ligne de compte[40]. Enfin, les analyses automatisées pouvant inévitablement comporter un certain taux d'erreurs, il importe de prévoir un réexamen individuel par des moyens non automatisés de tout résultat avant de déboucher sur une décision individuelle[41].

[36] J.-J. Oerlemans, M. Hagens et S. Royer, «Tijd voor een nieuwe bewaarplicht?», *Computerr.*, 2021, n° 2, pp. 151-159.

[37] *Ibid.*, p. 155 (notre traduction).

[38] *La Quadrature du Net*, préc., point 177-179. Voy. E. Daoud, I. Bello et O. Pecriaux, *op. cit.*, pp. 46 et s.

[39] *La Quadrature du Net*, préc., point 180. Voy. également, dans le même sens, C.J.U.E., avis 1/15, Accord PNR UE-Canada, 26 juillet 2017, point 172.

[40] *La Quadrature du Net*, préc., point 181.

[41] *Ibid.*, point 182. Le recours à l'intelligence artificielle a des conséquences qui font dire à Christophe Maubernard: «La Cour semble ici excessivement confiante dans la capacité de →

C. *Autres exceptions à la confidentialité des données de communication*

La Cour de justice a admis d'autres exceptions à la règle de la confidentialité des données de communication[42]. Elles sont toutefois moins larges que celles accordées au nom de la sécurité nationale.

Ainsi, s'agissant de la lutte contre la *criminalité grave*[43], un État peut prévoir la conservation ciblée des données de communication, délimitées en fonction de catégories de personnes visées ou de zones géographiques. La Cour de justice ne donne pas de balises de ce qu'elle entend par «criminalité grave», laissant aux États membres le soin d'en prévoir la portée, ce qui risque de conduire à des différences sensibles entre États européens[44]. Un État peut par ailleurs procéder à une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication, pour une durée de conservation limitée au strict nécessaire. En outre, conformément à ce qui est prévu dans la Convention de Budapest de 2001[45], la «conservation rapide» des données de trafic et de localisation est admise. Des autorités peuvent demander aux opérateurs de geler les données relatives à certaines personnes visées (suspects, victimes, entourage) si c'est nécessaire pour élucider des infractions pénales graves, que ces infractions soient déjà réalisées ou raisonnablement soupçonnées[46]. Cette conservation rapide ne peut se faire que pour que durée limitée au strict nécessaire, au maximum de 90 jours, mais éventuellement renouvelable[47].

←
l'humain à contrôler et encadrer une telle activité, à travers une série de conditions qui ont plutôt le visage de la 'méthode Coué' ou du performatif que de garanties effectives» (Chr. Maubernard, *op. cit.*, p. 579).

[42] Voy. A. Caiola, «Transmission et conservation des données en rapport avec la sécurité nationale: précisions et nuances», *R.A.E.-L.E.A.*, 2020, n° 4, p. 924.

[43] *La Quadrature du Net*, préc., points 140, 146 et s.

[44] En Belgique, si l'on doit s'appuyer sur l'article 90*ter* du Code d'instruction criminelle qui liste les quarante-cinq (catégories d')infractions justifiant l'interception de communications électroniques ou de données informatiques, cela ferait entrer dans la «criminalité grave», à côté d'infractions auxquelles on pense inévitablement (meurtres, enlèvements, empoisonnements, viols...) des infractions comme la production de fausse monnaie, la contrefaçon de timbres, l'attentat à la pudeur, le vol avec violence, la corruption privée, le recel... Selon Jan-Jaap Oerlemans, Mireille Hagens et Sofie Royer, cette liste «lijkt dus geen goede richtlijn meer voor wat precies ernstige criminaliteit is» (J.-J. Oerlemans, M. Hagens et S. Royer, *op. cit.*, p. 156).

[45] Article 16 de la Convention de Budapest du 23 novembre 2001 sur la cybercriminalité.

[46] *La Quadrature du Net*, préc., point 161.

[47] *Ibid.*, point 164.

D'autre part, afin de lutter contre la *criminalité en général*, un État peut procéder à une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs des moyens de communication électronique, sans que cela soit dans ce dernier cas limité à un délai particulier[48].

Dans toutes ces hypothèses, pour être admise, l'ingérence dans les droits fondamentaux doit respecter le principe de proportionnalité[49], être assortie de garanties effectives contre les abus et contrôlée par un juge ou une autorité administrative indépendante[50] [51].

IV. Décision de la Cour constitutionnelle belge dans la ligne de l'arrêt *La Quadrature du Net*

A. *Annulation de la loi et changement de perspective imposé au législateur*

La Cour constitutionnelle belge reprendra très largement le raisonnement de la Cour de justice. Elle relève que la directive 2002/58/CE, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, s'oppose à des mesures législatives imposant, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation[52]. Seules les hypothèses limitées décrites par la Cour de justice autorisent certaines formes de conservation de ces données. Ainsi, les règles européennes ne s'opposent pas à divers types de mesures législatives prévoyant cette conservation. Mais l'article 126, § 3, de la loi du 13 juin 2005 prévoit, par principe et sans limitation aux seules hypothèses listées dans l'arrêt *La Quadrature du Net*, une conservation généralisée et indifférenciée, par les opérateurs et fournisseurs de services de communications électroniques, des données d'identification, des données d'accès et de connexion, ainsi que des données de communication. Pour la Cour constitutionnelle, «[l]'arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix

[48] *Ibid.*, points 157-159.

[49] *Ibid.*, point 113.

[50] *Ibid.*, points 139 et 189.

[51] Sur l'exigence de proportionnalité et les garanties à respecter, voy. également Comité Européen de la Protection des Données, Recommandations 2/2020 sur les garanties essentielles pour les mesures de surveillance, adoptées le 10 novembre 2020, consultables à l'adresse https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_fr.

[52] Cour const., arrêt n° 57/2021, préc., B.15.

que le législateur a effectué: l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle»[53]. En outre, la loi du 13 juin 2005 présente aussi le défaut de poursuivre des objectifs plus larges que la lutte contre la criminalité grave ou contre le risque d'atteinte à la sûreté nationale. Faisant ce constat, la Cour constitutionnelle conclut que la loi belge viole les dispositions européennes ainsi que les articles 10 et 11 de la Constitution. En conséquence, elle annule les dispositions attaquées.

Dans la foulée de son raisonnement, la Cour donne des indications au législateur à propos de l'exercice qui l'attend de réécriture de la loi. Ainsi, la réglementation doit prévoir de manière claire et précise la portée de l'obligation de conservation des données, et doit imposer des exigences minimales garantissant que l'ingérence se limite au strict nécessaire et répond toujours à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi[54]. Moyennant le respect de plusieurs conditions, la législation peut distinguer certaines catégories de données faisant l'objet d'une obligation de conservation généralisée et indifférenciée: les adresses IP et les données relatives à l'identité civile des utilisateurs[55]. Selon la Cour, il ne s'agit pas là des catégories reprises à l'article 126, § 3, de la loi de 2005, contrairement à ce que prétendait le Conseil des ministres[56].

B. *Protection du secret professionnel*

L'Ordre des barreaux francophones et germanophone a plaidé devant la Cour constitutionnelle que, par sa généralité, l'obligation de conservation des données instaurée en Belgique couvre les personnes soumises au secret professionnel ainsi que les personnes ayant une obligation de confidentialité. Dès lors, les données collectées par les fournisseurs de services de téléphonie fixe et mobile, d'accès à internet et de courrier électronique permettent de déterminer si un avocat a été consulté par une personne physique ou morale, d'identifier les interlocuteurs et clients de cet avocat, ainsi que les dates et heures de ses communications[57]. Or, ces données devraient faire l'objet de garanties spéciales, vu l'obligation de secret qui y est normalement attachée. Mais la loi de 2005 traite de manière identique l'ensemble des utilisateurs de services de communication. Ce reproche est d'ailleurs formulé également par les professionnels comptables

[53] *Ibid.*, B.18.

[54] *Ibid.*, B.18, et *La Quadrature du Net*, préc., point 133.

[55] Cour const., arrêt n° 57/2021, préc., B.17 et B.19.

[56] *Ibid.*, B.16.1 et B.17.

[57] *Ibid.*, B.6.1.

et fiscaux qui relèvent que, eux aussi, alors qu'ils sont également soumis au secret professionnel, voient leurs données de communications enregistrées sans garanties spécifiques. Cette conservation généralisée des données impacte inévitablement la nécessaire relation de confiance qui doit unir ces professionnels à leurs clients[58].

La Cour fera écho à ces reproches en reprenant les affirmations de la Cour de justice[59] selon lesquelles la conservation et la transmission des données en question à des fins sécuritaires sont susceptibles, à elles seules, d'entraîner des effets dissuasifs sur l'exercice, par les utilisateurs des moyens de communication électronique, de leur liberté d'expression. Et la Cour relève que ces effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises au secret professionnel. La Cour constitutionnelle se contentera toutefois de ces affirmations et laissera au législateur le soin de déterminer les garanties qui répondront à cette préoccupation à l'égard des obligations légales de secret.

C. *Pas de maintien des effets de la loi*

Conformément à la réponse de la Cour de justice, la Cour constitutionnelle a refusé de prolonger les effets de la loi durant une période qui aurait permis de clôturer les affaires reposant sur des éléments de preuve liés aux données de communication exploitées par les services de police et de renseignement. Le Conseil des ministres avait demandé à la Cour d'accorder un tel délai afin de ne pas mettre en péril le travail de recherche et de poursuites des infractions. Mais la Cour de justice a été claire: il ne peut être question de maintenir temporairement les effets d'une législation nationale imposant aux fournisseurs de services de communications électroniques des obligations qui impliquent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été conservées[60].

Dans le même temps, la Cour de justice a rappelé que c'est au droit national qu'il appartient de déterminer l'admissibilité des preuves recueillies. Elle a toutefois précisé[61] que le juge pénal national devait écarter les preuves issues d'une

[58] *Ibid.*, B.7.1.

[59] *La Quadrature du Net*, préc., point 118, et *Privacy International*, préc., point 72.

[60] *La Quadrature du Net*, préc., point 222.

[61] *Ibid.*, point 228.

conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation mais seulement si les personnes soupçonnées n'ont pas été en mesure de commenter efficacement ces preuves susceptibles d'influencer de manière prépondérante l'appréciation des faits par le juge.

La Cour constitutionnelle a dès lors invité le juge pénal belge compétent à statuer sur cette admissibilité en tenant compte de l'éclairage équilibré apporté par la Cour de justice.

V. Décision du Conseil d'État français «tordant le raisonnement de la C.J.U.E.»[62]

Il était clair, au vu de ses questions préjudicielles[63], que le Conseil d'État français attendait de la Cour de justice, non pas tant qu'elle clarifie sa jurisprudence quant à la conservation des données de connexion mais plutôt qu'elle révise cette jurisprudence. La haute juridiction française, «prêtant l'oreille au discours sécuritaire»[64] tenu par le gouvernement français, était effectivement soucieuse de réexaminer l'équilibre entre liberté et sécurité afin de permettre aux autorités publiques le recours aux données de communication, devenu désormais la technique d'investigation privilégiée. La réponse de la Cour de justice, compromis sage[65] en faveur de la liberté même si des concessions sont accordées à la sécurité, n'était donc sans doute pas vraiment celle que le Conseil d'État espérait. Ce dernier[66] fera en conséquence de la «résistance»[67]. À la différence de la Cour constitutionnelle belge, il prendra de troublantes distances à l'égard de l'arrêt de la Cour de justice. Cette option évidemment délicate va

[62] Bastien Le Querrec, cité par B. LION, *op. cit.*

[63] C.E. (fr.), 26 juillet 2018, *La Quadrature du Net e.a.*, req. n° 394922, spéc. point 23.

[64] H. LABAYLE, «L'arrêt *French Data Network* du Conseil d'État: l'art d'une réponse contournée à des questions fondamentales», 1er juin 2021, *Institute for Digital Fundamental Rights*, consultable à l'adresse https://idfrights.org/larret-french-data-network-du-conseil-detat-lart-dunc-reponse-contournee-a-des-questions-fondamentales/.

[65] É. DUBOUT, «Le Conseil d'État, gardien de la sécurité», *Revue des droits et libertés fondamentaux* [en ligne], 2021, chron. n° 18, consultable à l'adresse www.revuedlf.com/droit-ue/le-conseil-detat-gardien-de-la-securite/.

[66] C.E. (fr.) (ass.), arrêt n° 393.099, préc.

[67] É. DUBOUT, *op. cit.*

déboucher sur une décision tout à la fois complexe, peu claire et discutable[68], alambiquée[69], iconoclaste[70], improbable et inquiétante[71].

A. *Limites à la primauté du droit de l'Union*

Le Conseil d'État statuant en Assemblée du contentieux, «sa formation la plus solennelle»[72], va refuser de suivre le gouvernement français qui l'invitait à déclarer que la Cour de justice a outrepassé ses compétences par son arrêt *La Quadrature du Net*[73]. Il va préférer la voie d'un positionnement sur la question de la hiérarchie des normes entre normes européennes telles qu'interprétées par la Cour de justice et norme constitutionnelle française. Pour lui, «en vertu des principes de primauté, d'unité et d'effectivité issus des traités, tels qu'ils ont été interprétés par la Cour de justice de l'Union européenne, le juge national, chargé d'appliquer les dispositions et principes généraux du droit de l'Union, a l'obligation d'en assurer le plein effet en laissant au besoin inappliquée toute disposition contraire, qu'elle résulte d'un engagement international de la France, d'une loi ou d'un acte administratif»[74]. Commençant donc diplomatiquement par donner des gages à la primauté du droit européen sur le droit national, le Conseil d'État poursuit toutefois en déclarant que «la Constitution

[68] H. Labayle, *op. cit.*

[69] É. Dubout, *op. cit.*

[70] Br. Bertrand, «L'arrêt *French Data Network* du Conseil d'État: un dialogue des juges en trompe l'œil», *Le club des juristes*, consultable à l'adresse https://blog.leclubdesjuristes.com/larret-french-data-network-du-conseil-detat-un-dialogue-des-juges-en-trompe-lœil/.

[71] P. Cassia, «Le Frexit sécuritaire du Conseil d'État», 23 avril 2021, consultable à l'adresse https://blogs.mediapart.fr/paul-cassia/blog.

[72] C.E. (fr.), Communiqué de presse «Données de connexion: le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité», 21 avril 2021.

[73] Pour davantage de développements sur cet aspect de la décision du Conseil d'État, voy. Jacques Ziller (J. Ziller, «Le Conseil d'État se refuse d'emboîter le pas au joueur de flûte de Karlsruhe», consultable à l'adresse https://blogdroiteuropeen.com/2021/04/23/) et Henri Labayle (H. Labayle, *op. cit.*) qui saluent cette position du Conseil d'État, tandis que Édouard Dubout et Brunessen Bertrand sont plus nuancés tout en reconnaissant «les raisons d'opportunité qui ont conduit le juge à ne pas ouvrir une telle brèche, *a fortiori* dans un contexte malheureux où elle pourrait aussi être instrumentalisée par la Pologne pour remettre en cause des valeurs européennes fondamentales» (Br. Bertrand, *op. cit.*), et le fait «qu'un contrôle national de l'*ultra vires* se développe n'est pas sans risque pour la poursuite de l'intégration européenne. Il fragilise la position de la Cour de justice comme interprète ultime et authentique du droit de l'Union, et le Conseil d'État y a été sensible» (É. Dubout, *op. cit.*).

[74] C.E. (fr.), *French Data Network e.a.*, préc., point 4.

française demeure la norme suprême du droit national»[75]. Il se donne dès lors pour mission de vérifier que le respect du droit européen tel qu'interprété par la Cour de justice ne compromet pas les exigences de la Constitution française, mais seulement celles qui ne sont pas protégées de façon équivalente par le droit européen[76].

Au titre de ces exigences constitutionnelles, le Conseil d'État parvient, par un raisonnement «particulièrement acrobatique»[77], à faire figurer la sécurité, estimant qu'elle est nécessaire à la sauvegarde des droits et libertés[78]. Ce qui fera dire au Professeur Paul Cassia que «de simples objectifs de valeur constitutionnelle 'valises' déduits de l'article 12 de la Déclaration de 1789 qui prévoit la nécessité d'une force publique sont consacrés au rang de règles et principes constitutionnels»[79]. Constituent ainsi des objectifs de valeur constitutionnelle: «[l]a sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, la lutte contre le terrorisme, ainsi que la recherche des auteurs d'infractions pénales»[80]. Or, selon le Conseil d'État, ces objectifs ne bénéficient pas sur le plan européen d'une protection équivalente à celle que garantit la Constitution française[81]. Ce constat lui permet d'intervenir pour veiller à ce que la protection offerte par la Constitution ne soit pas mise à mal par le droit européen. Ainsi qu'on le verra au paragraphe suivant, cela l'amènera sur plusieurs points à aménager le raisonnement de la Cour de justice.

[75] C.E. (fr)., Communiqué de presse précité; C.E. (fr.), *French Data Network e.a.*, préc., point 5.

[76] C.E. (fr.), *French Data Network e.a.*, préc., point 5; C.E. (fr)., Communiqué de presse, précité. Voy. F. Jault-Seseke, «Conservation des données de connexion: le Conseil d'État, option droit de l'Union européenne, un bon et habile élève», *Le club des juristes*, L'actualité au prisme du droit, 7 mai 2021, consultable à l'adresse https://blog.leclubdesjuristes.com/conservation-des-donnees-de-connexion-le-conseil-detat-option-droit-de-lunion-europeenne-un-bon-et-habile-eleve/.

[77] É. Dubout, *op. cit.*

[78] C.E. (fr.), *French Data Network e.a.*, préc., point 9.

[79] P. Cassia, *op. cit.* Voy. également Édouard Dubout pour qui la référence à la «force publique» mentionnée à l'article 12 de la Déclaration des droits de l'homme et du citoyen pour justifier la constitutionnalisation de la sécurité n'est pas convaincante. «Qu'une 'force publique' soit nécessaire à la garantie des libertés est une évidence, qu'elle fasse de la sécurité une finalité de la Constitution l'est beaucoup moins» (É. Dubout, *op. cit.*).

[80] C.E. (fr.), *French Data Network e.a.*, préc., point 9. Brunessen Bertrand relève que ces objectifs listés par le Conseil d'État «font partie du bloc de constitutionnalité mais ils ne sont pas non plus des droits et libertés constitutionnellement garantis. Malgré leur juridicité, leur portée normative et leur invocabilité restent limitées et il n'est pas sûr qu'ils puissent fonder un noyau dur d'exigences constitutionnelles» (Br. Bertrand, *op. cit.*).

[81] C.E. (fr.), *French Data Network e.a.*, préc., point 10.

C'est donc «[p]ar un exercice de prestidigitation»[82] que le Conseil d'État a donné l'impression de respecter le droit de l'Union sans pour autant appliquer complètement la leçon reçue dans la réponse de la Cour de justice aux questions qu'il lui avait posées.

On notera que, moins d'un mois après la décision française, c'est en se référant explicitement à l'arrêt *La Quadrature du Net,* que la Cour de Luxembourg a évoqué «le principe de primauté du droit de l'Union qui consacre la prééminence du droit de l'Union sur le droit des États membres»[83]. Et elle a ajouté, dans cet arrêt *Asociația Forumul Judecătorilor din România*, que «le fait pour un État membre d'invoquer des dispositions de droit national, *fussent-elles d'ordre constitutionnel*, ne saurait porter atteinte à l'unité et à l'efficacité du droit de l'Union»[84].

B. *Limites à l'équilibre libertélsécurité dicté par la Cour de justice*

Le Conseil d'État va donc se permettre des écarts par rapport à la leçon de l'arrêt *La Quadrature du Net.*

Ainsi, tout d'abord, il donne de la notion de sécurité nationale une définition particulièrement large puisqu'à ses yeux, elle recouvre les intérêts fondamentaux de la Nation énumérés à l'article L.811-3 du Code de la sécurité intérieure[85], ceux figurant au titre Ier du livre IV du Code pénal, ainsi que le

[82] Br. Bertrand, *op. cit.* Brunessen Bertrand relève en outre que «le communiqué de presse [dans lequel le Conseil d'État annonce qu'il concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité] va sans doute un peu loin dans le jeu des apparences».

[83] C.J.U.E., arrêt *Asociația Forumul Judecătorilor din România e.a.*, 18 mai 2021, aff. jtes n° C-83/19, n° C-127/19, n° C-195/19, n° C-291/19, n° C-355/19 et n° C-397/19, point 244.

[84] *Ibid.*, point 245 (c'est nous qui soulignons). C'était sans doute l'occasion aussi de le rappeler aux hautes juridictions allemande et polonaise...

[85] Article L.811-3 du Code de la sécurité intérieure: «*Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants: 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale; 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère; 3° Les intérêts économiques, industriels et scientifiques majeurs de la France; 4° La prévention du terrorisme; 5° La prévention: a) Des atteintes à la forme républicaine des institutions; b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1;* →

terrorisme[86]. Cela signifie que l'objectif de sauvegarde de la sécurité nationale peut être invoqué notamment pour des objectifs flous comme la défense des engagements européens et internationaux de la France, la protection des intérêts économiques et scientifiques majeurs de la France, ou la prévention des violences collectives. Par ailleurs, le Conseil d'État estime que, depuis 2015 jusqu'à l'heure de sa décision, la conservation généralisée des données a bien été justifiée, comme l'exige la Cour de justice, par une menace pour la sécurité nationale, menace grave et réelle, «non seulement prévisible mais aussi actuelle»[87], qui prend la forme de menace terroriste, risque d'ingérence étrangère et d'espionnage (y compris industriel et scientifique), et de menace pour la paix publique provenant de groupes radicaux et extrémistes[88]. En revanche, il reproche l'absence de réévaluation périodique de la persistance de cette menace et accorde six mois au gouvernement pour se conformer aux exigences européennes et prévoir un réexamen au moins annuel de la menace[89]. Il enjoint aussi au gouvernement de subordonner à l'autorisation d'une autorité indépendante l'accès et l'exploitation par les services de renseignement des données conservées[90].

Ensuite, s'il juge illégale, dans la ligne de l'arrêt *La Quadrature du Net*, l'obligation de conservation généralisée des données (à l'exception des données relatives à l'état civil, aux comptes et aux paiements ainsi que de l'adresse IP) à des fins autres que la sécurité nationale et la lutte contre le terrorisme, il déploie un raisonnement dont le pragmatisme surprend, pour ne pas priver les autorités luttant contre la criminalité grave de l'accès aux données de connexion.

←

c) Des violences collectives de nature à porter gravement atteinte à la paix publique; 6° La prévention de la criminalité et de la délinquance organisées; 7° La prévention de la prolifération des armes de destruction massive».

[86] C.E. (fr.), *French Data Network e.a.*, préc., point 43, également point 67.

[87] *Ibid.*, point 44.

[88] *Ibid.*, points 44, 66 et 96.

[89] *Ibid.*, point 45. Pour Bastien Le Querrec, «cette clause de revoyure est purement de façade [...] il s'agit là d'un acte administratif qui sera pris par le Premier ministre et qui ne comportera absolument aucun contrôle ni du Parlement ni de la CNCTR. [...] En l'état, nous n'avons aucun contrôle en dehors des affirmations des services de renseignement» (Bastien Le Querrec, cité par B. Lion, *op. cit.*).

[90] C.E. (fr.), *French Data Network e.a.*, préc., points 68 à 74. Cette exigence avait déjà été formulée dans l'arrêt de la Cour de justice *Tele2 Sverige* du 21 décembre 2016, précité. Le Conseil d'État note que si, dans son arrêt du 6 octobre 2020, la Cour n'a rappelé cette exigence d'un contrôle préalable par une autorité indépendante qu'à propos du recueil en temps réel des données de connexion par les services de renseignement, elle a par contre bien réitéré le principe du contrôle préalable de l'accès des autorités nationales aux données de connexion dans son arrêt du 2 mars 2021, *H.K. c. Prokuratuur* (aff. C-746/18).

Ainsi, il estime que la méthode de «conservation rapide» autorisée par la Convention sur la cybercriminalité, consistant à geler les données pour une durée de maximum 90 jours renouvelable, peut «s'appuyer sur le stock de données conservées de façon généralisée pour les besoins de la sécurité nationale, et peut être utilisée pour la poursuite des infractions pénales»[91]. C'est donc une étonnante solution bancale que propose le Conseil d'État, reposant sur l'existence d'un stock de données constitué en réponse à une menace grave pour la sécurité nationale, dans lequel les autorités pourront venir puiser pour combattre un objectif voisin – la criminalité grave –, solution qui s'écroulerait dès que cette menace disparaîtrait, et avec elle la mine d'informations. On pourrait en conclure que soit la juridiction française est persuadée que la menace ne disparaîtra pas de sitôt, voire jamais[92], soit elle souhaite «temporiser une situation, qui, de toute façon, est appelée à évoluer avec l'adoption proche du règlement *e-privacy*»[93]. Le législateur européen est en effet engagé depuis des années dans la révision de la directive 2002/58/CE relative à la protection des données dans les communications électroniques en vue de la mettre à jour en la transformant en un règlement *e-privacy*. Le sort des données de connexion est sans doute à l'ordre du jour des discussions les plus intenses au Conseil et au Parlement de l'UE…

Quant à la méthode alternative de conservation ciblée plutôt qu'indifférenciée des données, également préconisée par la Cour de justice pour la lutte contre la criminalité grave, le Conseil d'État la juge ni matériellement praticable, ni opérationnellement efficace[94]. Selon lui, une conservation ciblée ne permet pas d'accéder aux données de connexion de personnes tels les primo-délinquants qui n'auraient pas été préalablement identifiés comme susceptibles de commettre une infraction ou de personnes qui ont recours à des téléphones munis de cartes prépayées non identifiées. Par ailleurs, une obligation de conservation des données de connexion limitée à certaines zones géographiques fait obstacle à l'action des services d'enquête dans les autres parties du territoire où des infractions pourraient être commises. En outre, pour le Conseil d'État, retenir une présomption de dangerosité à l'encontre de personnes en fonction de leur lieu de résidence ou d'activité professionnelle pour justifier la conservation de

[91] C.E. (fr.), Communiqué de presse et arrêt préc., points 55 et 57.

[92] F. JAULT-SESEKE, *op. cit.*

[93] Br. BERTRAND, *op. cit.*

[94] C.E. (fr.), *French Data Network e.a.*, préc., point 54. Il est à noter que le législateur belge avait aussi estimé qu'il n'était pas possible de procéder à une différenciation *a priori* en fonction des personnes, des périodes temporelles et des zones géographiques (Cour const., arrêt n° 57/2021, préc., B.4).

leurs données de trafic et de localisation serait contraire au principe d'égalité devant la loi.

Enfin, concernant les adresses IP, le Conseil d'État est d'avis qu'il ne faut pas modifier la solution française qui prévoit pourtant leur conservation généralisée et indifférenciée sans que ce soit limité aux seuls besoins de la sécurité publique et de la lutte contre la criminalité grave. La haute juridiction se contente du principe de proportionnalité énoncé à l'article préliminaire du Code de procédure pénale (imposant la proportionnalité entre le recours à des mesures portant atteinte à la vie privée d'une personne et la gravité de l'infraction commise par cette personne) pour garantir que seules les infractions pénales présentant un degré de gravité suffisant pour justifier l'ingérence dans les droits des individus permettront l'accès des services d'enquêtes aux adresses IP conservées par les opérateurs. Que cela ne soit pas plus clairement formulé dans la législation ne trouble pas le Conseil d'État, pas plus que le fait que le législateur n'ait pas défini les catégories d'infractions relevant de la criminalité grave et que celles-ci doivent donc s'apprécier de façon concrète en tenant compte des circonstances.

En guise de conclusion

La question de l'équilibre entre sécurité et liberté à redéfinir dans le contexte technologique d'aujourd'hui est à l'agenda des plus hautes juridictions sur le continent européen. Ainsi, sept mois après la Cour de justice et un mois après le Conseil d'État français et la Cour constitutionnelle belge, la Cour européenne des droits de l'homme s'est à son tour prononcée, en Grande Chambre, sur la question de la conservation massive des données de communication. À l'occasion de deux affaires, respectivement contre le Royaume-Uni[95] et contre la Suède[96], la Cour de Strasbourg a considéré que les États jouissent d'une ample marge d'appréciation pour déterminer le régime d'interception des données dont ils ont besoin pour protéger leur sécurité nationale. La Cour n'estime donc pas le recours à un régime d'interception en masse en soi contraire à l'article 8 de la Convention européenne des droits de l'homme. Mais pour que ce régime soit acceptable, étant donné le risque d'abus inhérent à ce type d'interception, la Cour estime qu'il doit être encadré par des «garanties de bout en bout». Ces garanties consistent à évaluer à chaque étape du processus la nécessité et la proportionnalité des mesures prises, et à soumettre les inter-

[95] Cour eur. dr. h., Gde Ch., arrêt *Big Brother Watch e.a. c. Royaume-Uni*, 25 mai 2021.

[96] Cour eur. dr. h., Gde Ch., arrêt *Centrum för rättvisa c. Suède*, 25 mai 2021.

ceptions, en amont, à l'autorisation d'une autorité indépendante et, en aval, à un contrôle indépendant. Dans des opinions jointes aux arrêts, plusieurs juges ont estimé que la Cour « aurait dû aller bien plus loin dans la réaffirmation de l'importance de la protection de la vie privée et de la correspondance »[97] et que « la Cour de Strasbourg reste en retrait de la Cour de Luxembourg »[98]. Pour le juge Pinto de Albuquerque, l'arrêt *Big Brother* de la Cour européenne des droits de l'homme « ouvre la voie à un 'Big Brother' électronique en Europe »[99].

Il est clair que la prolifération des menaces que font aujourd'hui peser sur les États des réseaux d'acteurs internationaux qui œuvrent via internet et recourent à des technologies sophistiquées pour échapper à la détection appelle une réponse adaptée. La Cour de justice a veillé à nuancer sa réponse, dans son arrêt *La Quadrature du Net*, en fonction des enjeux de protection de la sécurité nationale, de lutte contre la criminalité grave ou contre la criminalité ordinaire. Si elle a assoupli sa position par rapport à sa jurisprudence antérieure, elle n'a pas abdiqué son rôle de « phare de la protection de la vie privée en Europe »[100]. Son message équilibré porte bien au-delà des frontières belges et françaises des États qui l'avaient saisie. Il s'adresse aussi aux États membres tentés par la surveillance des communications électroniques des citoyens, journalistes, avocats, politiciens, et autres activistes. L'histoire et l'actualité démontrent qu'il est dangereux de se draper dans une tradition démocratique qui mettrait à l'abri de tout dérapage[101].

À Bruxelles, les juges nationaux se sont loyalement alignés sur la décision de la Cour de justice tandis qu'ils ont fait preuve, à Paris, de résistance semi-larvée. La tâche est désormais bien plus ardue pour le législateur belge devant remettre l'ensemble de l'ouvrage sur le métier que pour le législateur français qui s'est vu octroyer six mois pour faire des modifications cosmétiques à ses textes. Le législateur européen ne manquera pas non plus d'intervenir, par le

[97] P. Lemmens, F. Vehabović et M. Bošnjak, opinion concordante commune sous Cour eur. dr. h., Gde Ch., *Centrum för rättvisa c. Suède*, préc.

[98] P. Pinto de Albuquerque, opinion concordante sous Cour eur. dr. h., Gde Ch., *Centrum för rättvisa c. Suède*, préc.

[99] *Ibid.*, § 60.

[100] *Ibid.*

[101] On ne suivra donc pas le rapporteur public français qui dénonce « une logique de méfiance à l'égard des autorités publiques, qu'il faut se garder de soumettre à la tentation, [...] : c'est le spectre de la surveillance de masse et de l'intrusion permanente dans la « vie des autres », [...] que la bonne science-fiction s'est employée à transposer dans un avenir qui pourrait être le nôtre. [...] Il est bien entendu permis de penser, alternativement, que les forces de sécurité de ce pays consacrent les moyens qu'on leur donne à protéger les Français plutôt qu'à les espionner » (rapp. publ. A. Lallet, conclusions précédant C.E. (fr.), *French Data Network e.a.*, préc., p. 16).

biais de son règlement *e-privacy*[102], qui devrait bientôt remplacer la directive 2002/58/CE relative à la protection des données dans les communications électroniques.

[102] Proposition de règlement du Parlement européen et du Conseil du 10 janvier 2017 concernant le respect de la vie privée des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »).