# La conservation des données de connexion, le droit français et la Cour de justice de l'Union européenne. Quelles conséquences pour les enquêtes judiciaires.

Matthieu Audibert

s'applique. Sur les textes réglementaires, le Conseil d'Etat devra trancher. L'arrêt crée une instabilité juridique considérable et néglige le fait que la protection du citoyen contre la criminalité est un objectif à valeur constitutionnelle.
L'analyse faite ci-après par Matthieu Audibert est suffisamment éclairante pour faire prendre conscience des conséquences graves d'un arrêt « hors-sol ».

*Capitaine Matthieu AUDIBERT*

## La conservation des données de connexion
## Le droit français et la Cour de justice de l'Union européenne
## Quelles conséquences pour les enquêtes judiciaires ?

À l'heure actuelle, le droit français prévoit un cadre juridique précis pour la conservation généralisée et indifférenciée des données techniques de connexion[3] et des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne[4].
L'article L. 34-1 III du Code des postes et des communications électroniques (CPCE) dispose que *« pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales (…), il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines*

3. Article L 34-1 III du Code des postes et des communications électroniques.
4. Article 6 II de la loi n° 2004-575 du 21 juin 2004, Loi pour la confiance dans l'économie numérique (LCEN).

*catégories de données techniques. (…)»*.

Ces données techniques sont détaillées à l'article R. 10-13 du même Code. Ainsi, *« (…) les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales : les informations permettant d'identifier l'utilisateur ; les données relatives aux équipements terminaux de communication utilisés; les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs; les données permettant d'identifier le ou les destinataires de la communication »*. Ce même article prévoit que les opérateurs conservent les données susmentionnées pour les activités de téléphonie mais aussi celles permettant d'identifier l'origine et la localisation de la communication. Cette durée de conservation des données est d'un an à compter du jour de l'enregistrement.

S'agissant des contenus publiés sur Internet, l'article 6 II de la Loi pour la confiance dans l'économie numérique (LCEN) dispose que *« les personnes mentionnées aux 1 et 2 du I [fournisseurs d'accès à internet et hébergeurs] détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires »*.
Le 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 vient préciser les données qui doivent être conservées.

## Droit de l'espace numérique

Les données visées ici sont appelées données techniques de connexion. En pratique, il s'agit de métadonnées liées aux communications électroniques et de métadonnées liées à la création de contenus sur Internet.

Plusieurs associations, dont la Quadrature du Net, ont contesté devant le Conseil d'État la légalité de la réglementation française rappelée *supra* en attaquant les dispositions réglementaires de celle-ci. Ces associations estiment que ces dispositions réglementaires sont non conformes à la directive 2002/58/CE *ePrivacy* telle qu'interprétée par la CJUE dans son arrêt rendu le 21 décembre 2016 dans l'affaire *Tele 2 Sverige*. Afin de pouvoir statuer, le Conseil d'État a saisi la Cour de justice de l'Union européenne (CJUE) de plusieurs questions préjudicielles[5], qui ont été jointes à des affaires britannique et belge et sur lesquelles la Cour s'est prononcée le 6 octobre 2020.

S'agissant des enquêtes judiciaires, le Conseil d'État a posé les questions préjudicielles suivantes :

- *« L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive [2002/58], ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la*

5. Conseil d'État, 6 septembre 2018, n° 394922.

*sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE] ? »*

*- « Les dispositions de la directive [2000/31], lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la [Charte], doivent-elles être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ? »*

Saisie de ces questions préjudicielles, la CJUE va alors se livrer à un contrôle de proportionnalité entre, d'une part, l'objectif d'intérêt public poursuivi par la législation française et, d'autre part, l'atteinte au droit des personnes.[6]

6. CRICHTON Céline, Conservation de données à des fins de sécurité nationale et de lutte contre la criminalité : la CJUE rend ses arrêts, *Dalloz actualité*, 13 octobre 2020. Disponible sur : https://www.dalloz-actualite.fr/flash/conservation-de-donnees-des-fins-de-securite-nationale-et-de-lutte-contre-criminalite-cjue-ren#.X79dj2hKiUk

## La conservation des données de communication aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique

La Cour note que, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, *« seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux (…), telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation »*[7].
Or, la Cour considère qu'une telle conservation *« excède les limites du strict nécessaire »*. En effet, cette conservation n'est pas justifiée, car elle vise la totalité des utilisateurs pour le seul objectif de lutte contre la « criminalité grave » et de prévention des menaces graves contre la sécurité publique[8].

La Cour énonce ensuite ce qui serait admissible, à savoir une mesure prévoyant *« à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation »*. Celle-ci doit être limitée au strict nécessaire *« en ce qui concerne les catégories de données à conserver, les moyens de communication visées, les personnes concernées ainsi que la durée de conservation retenue »*[9].
La Cour précise deux options envisageables : tout d'abord des

7. Point 140 de l'arrêt.
8. Points 141-143.
9. Point 147.

personnes qui auraient été *« préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné »*[10], enfin une délimitation fondée sur un critère de zone géographique *« lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave »*[11].

## La conservation des adresses IP et des données relatives à l'identité civile aux fins de lutte contre la criminalité et de la sauvegarde de la sécurité publique

Sur ce point, la solution de la CJUE est différente par rapport à la conservation généralisée et indifférenciée des données de connexion. En effet, elle estime proportionnée une législation nationale prévoyant la conservation par les fournisseurs de services de communications électroniques de données relatives à l'identité civile de l'ensemble de ses utilisateurs aux fins de la prévention, de la recherche, de la détection et de la poursuite des infractions pénales[12]. Il convient de souligner que, pour la Cour, la notion de gravité de l'infraction ou de la menace est indifférente, la seule connaissance de l'identité des utilisateurs de ces services ne constituant pas une ingérence grave dans leurs droits.

10. Point 149.
11. Point 150.
12. Points 157-159.

Pour la conservation de l'adresse IP, la Cour adopte une position plus restrictive : sa conservation constitue une ingérence grave dans les droits des utilisateurs[13]. À cet égard, reprenant le principe de proportionnalité, la Cour indique que seule sa conservation dans un objectif de lutte contre la criminalité ou de prévention des menaces graves contre la sécurité publique est de nature à justifier une telle ingérence dans les droits et libertés des utilisateurs[14]. Elle reprend ensuite les garanties évoquées précédemment, fondées sur une limitation dans le temps et une conservation strictement nécessaire.

## La conservation rapide des données de connexion et de localisation aux fins de lutte contre la « criminalité grave »

Ici, l'hypothèse visée est celle d'une infraction commise et constatée ou, comme le souligne la Cour, dont l'*« existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée »*[15]. La Cour juge ainsi qu'il est possible de prévoir un cadre juridique national permettant d'enjoindre aux fournisseurs de services de communications électronique de conserver ces données[16]. Là encore, cette conservation doit répondre à l'objectif de lutte contre la « criminalité grave » et cette mesure doit être limitée dans le temps.

---

13. Point 153.
14. Points 154-156.
15. Point 160.
16. Point 163.

Sur ce point, la CJUE évoque la conservation rapide de données informatiques stockées telle que prévue par l'article 17 de la Convention de Budapest[17]. Ce dispositif a fait l'objet d'une transposition partielle en droit français[18], la conservation des données de trafic et de localisation étant prévue par d'autres dispositions de droit national, notamment dans le Code des postes et des communications électroniques.

## La conservation généralisée et indifférenciée des données par les fournisseurs d'accès à des services de communication au public en ligne et par les fournisseurs de services d'hébergement

Comme nous l'avons vu précédemment, cette conservation est fondée sur la LCEN et le décret n° 2011-219 du 25 février 2011.
Pour la CJUE, la directive 2000/31/CE du 8 juin 2000 sur le commerce électronique n'est pas applicable au litige[19]. Ici ce sont la directive *ePrivacy* 2002/58/CE et, le cas échéant, le Règlement général sur la protection des données (RGPD) qui sont applicables[20]. Cette directive s'applique aux services d'accès à Internet et aux services de messagerie sur Internet, dès lors qu'ils impliquent entièrement ou principalement la transmission de signaux sur des réseaux de communication électronique[21].

17. Article 17 de la Convention sur la cybercriminalité dite de Budapest du 23 novembre 2001.
18. Article 60-2 alinéa 2 du Code de procédure pénale.
19. Points 197-199.
20. Points 200-201.
21. Points 204-205.

Ainsi, deux options se présentent :

- Si les données en cause sont soumises à la directive *ePrivacy*, la Cour renvoie à sa position, s'agissant de la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation[22];
- Si le traitement de ces données constitue un traitement de données à caractère personnel, c'est le RGPD qui s'applique et ce dernier s'oppose à une réglementation prévoyant que les fournisseurs d'accès à Internet et les hébergeurs soient contraints de conserver de manière généralisée et indifférenciée ces données[23].

## Le juge national et l'arrêt de la CJUE

Une question était posée à la Cour concernant la possibilité pour un juge national de différer dans le temps l'application de l'arrêt de la CJUE par rapport au droit national en vigueur. La Cour répond ici, qu'en vertu du principe de primauté, le juge national est chargé d'assurer le plein effet du droit de l'UE *« en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel »*[24].

Ainsi, le juge national ne peut pas limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, s'agissant d'une législation nationale prévoyant la conservation généralisée et

22. Point 203.
23. Points 213-228.
24. Point 215.

indifférenciée des données[25].

La Cour conclut : le juge national doit écarter *« des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits »*[26].

**Après avoir présenté les grandes lignes de cet arrêt, quelles en sont les conséquences pour les enquêtes judiciaires ?**

Premier constat : si la CJUE parle dans son arrêt de la possibilité de recourir à une conservation ciblée des données, elle ne l'envisage que pour la « criminalité grave » ou la prévention des menaces graves contre la sécurité publique. Cette notion de gravité n'est pas définie dans la jurisprudence de la CJUE.
En droit français, les infractions sont classées en trois catégories : contravention, délit et crime avec, pour chacune, des échelles de sanctions différentes. On pourrait en déduire qu'un crime est nécessairement grave mais qu'un délit ne l'est pas. Or, si l'on prend

25. Points 216-220.
26. Points 221-226.

l'exemple d'un délit souvent constaté sur Internet, le cyberharcèlement, celui-ci est puni de deux ans d'emprisonnement et de 30 000€ d'amende[27]. Est-ce une infraction grave ? Pour la victime certainement mais pour l'ordre public ? L'actualité récente nous indique que des faits de cyberharcèlement peuvent déboucher sur des atteintes réelles à l'intégrité physique.
Autre exemple, les atteintes aux mineurs sur Internet (propositions sexuelles, diffusion de l'image d'un mineur présentant un caractère pornographique, etc.) sont des délits et non des crimes[28]. Or, sont-elles des infractions graves ?

Comme le souligne le colonel Éric Freyssinet sur son blog[29], il n'existe à ce jour aucune définition dans le droit de l'Union européenne ou dans le droit français de ce qui relèverait de la « criminalité grave » telle que l'entend la CJUE dans son arrêt. Dans notre droit national, seule l'échelle des peines peut constituer un éventuel indicateur mais comme cela a été expliqué précédemment : peut-on considérer qu'un délit commis sur Internet n'est pas une infraction grave ? Le seul texte explicitant la notion d'infraction grave est la Convention de Palerme relative à la lutte contre le crime transnational organisé adoptée en 2004. Son article 2 b) dispose qu'une infraction grave *« désigne un acte constituant une infraction passible d'une peine privative de liberté dont le*

27. Article 222-33-2-2 du Code pénal.
28. Articles 227-22-1 et 227-23 du Code pénal.
29. FREYSSINET Éric, Décision de la CJUE du 06/10/2020 sur les données de connexion, *Investigation & transformation numériques* (*blog*), 9 octobre 2020. Disponible sur : https://eric.freyssi.net/2020/10/09/decision-de-la-cjue-du-06-10-2020-sur-les-donnees-de-connexion/

*maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde »*.

On constate ici que c'est l'échelle des peines qui détermine la gravité de l'infraction et non l'atteinte qu'elle est censée réprimer. Dès lors, il serait aisé de modifier l'échelle des peines mais cela ne saurait être une solution satisfaisante, le problème ne consistant pas réellement dans cette notion de « criminalité grave » mais plutôt dans l'absence de conservation de données antérieures à la commission.

En réalité, la liste des délits aggravés par *« l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique »* est extrêmement longue et les investigations sur ces infractions vont être rendues difficiles, presque impossibles avec cet arrêt de la CJUE.

De nombreuses infractions sont commises exclusivement sur Internet ou, en tout cas, par l'utilisation d'un moyen de communication électronique. Pour reprendre les infractions citées *supra*, si la CJUE admet la conservation de l'adresse IP et des identités civiles associées[30], comment faire le lien entre l'équipement terminal et l'adresse IP au moment de la commission des faits ? En pratique ce sera impossible.

Illustration : un individu publie des contenus illicites sur le réseau social Twitter. Un enquêteur constate immédiatement l'infraction

30. Points 152 à 160.

et ouvre une enquête de flagrance[31]. Il constate que le message a été diffusé via une application pour smartphone. Il émet ensuite une réquisition à Twitter[32] pour solliciter la communication des données de connexion concernant le compte ayant diffusé ces contenus. La société Twitter répond en communiquant l'adresse email ou le numéro de téléphone utilisé au moment de la création du compte ainsi que l'adresse IP.
L'enquêteur peut alors identifier le titulaire du compte et son fournisseur d'accès à Internet. Toutefois, comment faire le lien avec le suspect ? En effet, en l'absence de conservation des données de connexion par le fournisseur d'accès (i.e. l'opérateur téléphonique), il serait impossible d'affirmer de manière certaine que c'est de ce téléphone que le suspect s'est connecté tel jour à telle heure sur le réseau social et a publié ce message.

Autrement dit, l'imputation du message sera quasi impossible à prouver puisque les données de connexion seront absentes.

Au-delà des faits commis sur Internet, la conservation des données de connexion est aussi nécessaire pour élucider des enquêtes complexes.

Prenons un autre exemple, s'agissant d'un dossier criminel qui sera bientôt jugé. Dans la nuit du 11 au 12 avril 2017, un individu disparaît à Chambéry. La nuit de sa disparition, son téléphone a été localisé dans le centre-ville puis à 6 km de là. Le 7 septembre 2017,

31. Article 53 du Code de procédure pénale.
32. Article 60-1 du Code de procédure pénale.

un promeneur découvre les restes d'un crâne humain. Plusieurs mois après ces faits, dans une autre enquête criminelle dont les faits ont été commis à plusieurs kilomètres, les enquêteurs ont identifié un suspect. Travaillant sur la téléphonie et l'historique des données de connexion et de localisation (via les relais téléphoniques), ils constatent que le téléphone du suspect a déclenché les mêmes antennes relais que le téléphone de l'individu qui a disparu en avril 2017. Le suspect sera mis en examen dans le cadre de ce dossier.

Que retenir de ce second exemple ?
Sans les données de connexion et de localisation nécessairement antérieures à la commission des faits que les opérateurs conservent en vertu des dispositions législatives et réglementaires en vigueur, il aurait été impossible de faire le lien entre ces deux dossiers, quand bien même une conservation ciblée aurait pu être demandée, la clé des investigations résidant dans les données de connexion antérieures à la découverte des faits.

Que faut-il en conclure ?

Cet arrêt de la CJUE ne peut que soulever une vive inquiétude[33]. Comme le souligne le procureur François Molins[34], *« à l'exception*

33. BERLIN Dominique, La Cour de justice revient sur l'interdiction absolue des mesures générales de conservation et de traitement des données à caractère personnel, pour finalement en dresser le régime dérogatoire, *Juris-Classeur périodique, édition générale (JCP G)*, n° 48, 23 novembre 2020.

34. MOLINS François, La protection des citoyens européens dans un monde ultra-connecté, Fondation Robert Schuman, *Questions d'Europe*, n° 510, 8 avril 2019. Disponible sur : https://www.robert-schuman.eu/fr/questions-d-europe/0510-la-protection-des-citoyens-europeens-dans-un-monde-ultra-connecte

*des enquêtes pour association de malfaiteurs visant des objectifs nominatifs, il n'y a pas de crime dont on connaîtrait préalablement les auteurs et dont la conservation des données pourrait être ordonnée. Ce n'est bien évidemment qu'a posteriori, une fois les premiers éléments d'enquête recueillis, que la consultation des données conservées va être effectuée. S'il n'y a pas de données conservées préalablement, il n'y a pas de consultation »*.

Il poursuit en indiquant que *« sans conservation préalable des données, il n'est pas possible, après un fait criminel grave tel un acte terroriste, de croiser les connexions entre les personnes impliquées et dès lors d'établir leur participation aux faits ou d'identifier leurs complices et de démanteler les réseaux »*.

Dans un monde de plus en plus connecté et dans lequel le numérique prend de plus en plus de place, il semble impossible de se passer des données de connexion pour lutter contre la délinquance. En 1996, le Conseil constitutionnel déclarait que *« la recherche des auteurs d'infractions est nécessaire à la sauvegarde de principes et droits de valeur constitutionnelle »*[35].
Toutefois, il ne faut pas opposer la protection de la vie privée à la recherche des auteurs d'infractions. Il faut concilier ces deux impératifs. Le choix à privilégier aurait pu être celui de la conservation des données dont l'accès est garanti par le contrôle juridictionnel d'un magistrat indépendant.

35. Conseil constitutionnel, DC n° 96-377 du 16 juillet 1996, §16.