L'enjeu de la conservation des données de connexion

Matthieu Audibert

L'enjeu de la conservation des données de connexion

Par Matthieu Audibert
Officier de gendarmerie
Doctorant en droit privé et sciences criminelles
CDPC – EA 3982

« *A l'ère numérique, la protection de la vie privée et des données à caractère personnel est une des garanties essentielles de nos libertés. Mais celle-ci doit être si absolue, ou ses limites doivent-elles être si contraintes, qu'elle primerait de fait sur la capacité des autorités publiques à protéger le droit à la sûreté et donc l'exercice de toutes les libertés ?* [1] ».

Les données de connexion, parfois appelées, métadonnées sont un ensemble de données techniques qui doivent être différenciées des données dites « de contenu ». Ces données techniques permettent de renseigner sur l'utilisation d'un support numérique connecté à un réseau de téléphonie mobile ou à un fournisseur d'accès à Internet. A l'inverse, les données de contenu comprennent comme leur nom l'indique la teneur ou le contenu des conversations, des données échangées. Par analogie avec un courrier postal, les données de connexion concernent l'enveloppe, les données de contenu concernent ce qui est dans l'enveloppe.

Il est possible de distinguer trois catégories de données de connexion[2] :

- Les données d'identification : elles permettent de savoir a priori qui est titulaire d'un numéro de téléphone, d'un numéro de carte SIM, d'une adresse email, d'une adresse IP ;
- Les données de trafic : elles renseignent sur l'utilisation du support numérique connecté. Il s'agit des factures détaillées, de la liste des contacts appelés, de la durée des appels, des appareils utilisés, de l'historique de l'envoi et de la réception des emails, la liste des adresses IP consultées à partir d'une adresse ;
- Les données de localisation : ce sont les zones d'émission et de réception d'une communication, la liste des appels ayant transité par une antenne relais, la localisation des téléphones portables en veille grâce aux déclenchements des relais téléphoniques.

Ces données sont donc par nature extrêmement sensibles puisqu'elles peuvent renseigner sur les habitudes d'un utilisateur, elles permettent de reconstituer un parcours ou encore de déterminer ses interlocuteurs. C'est la raison pour laquelle les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonymes ces données relatives aux communications électroniques.[3]

Toutefois, à l'ère du tout numérique et à une époque où plus de 99% de la population âgée de 15 ans ou plus est équipée d'un téléphone, fixe ou mobile[4], ces mêmes données représentent un ensemble d'informations extrêmement précieuses pour la recherche

1 F. Molins, *La protection des citoyens européens dans un monde ultra-connecté*, Fondation Robert SCHUMAN, Question d'Europe, n°510, 8 avril 2019

2 Articles R. 10-12 à R. 10-14 du code des postes et des communications électroniques

3 Article L. 34-1 II du code des postes et des communications électroniques

4 INSEE Focus, n°259, 24 janvier 2022

d'auteurs d'infractions et apporter des réponses à la détresse des victimes. A cet égard, la loi prévoit notamment une exception à la suppression des données de connexion.
Ainsi, les opérateurs de communications électroniques sont tenus de conserver pour les besoins des procédures pénales les informations relatives à l'identité civile de l'utilisateur[5], les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement[6]. Pour les besoins de la lutte contre la criminalité et la délinquance grave, ils conservent les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés[7].

En outre, pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constaté une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic[8] en complément de celles déjà conservées[9].

Ce cadre juridique complexe témoigne de l'extrême sensibilité que revêt la conservation des données de connexion. En effet il s'agit de concilier d'une part le droit au respect de la vie privée, principe à valeur constitutionnelle[10], et d'autre part la recherche des auteurs d'infraction, objectif de valeur constitutionnelle[11].

Or les décisions récentes de la Cour de justice de l'Union européenne (CJUE)[12] ont entraîné de profondes inquiétudes chez les enquêteurs[13] et chez certains auteurs[14].
Dès lors, de la conservation à l'accès aux données de connexion, quel pourrait-être ce nouvel équilibre, respectueux des droits et libertés et permettant d'identifier, de rechercher et de poursuivre les auteurs d'infractions ?

Considérant les réalités opérationnelles et l'état des cybermenaces, il apparait nécessaire de maintenir une conservation généralisée et indifférenciée des données de connexion (I) tout en renforçant les modalités relatives à leur accès (II).

---

5 Article L. 34-1 II bis 1° du code des postes et des communications électroniques
6 Article L. 34-1 II bis 2° du code des postes et des communications électroniques
7 Article L. 34-1 II bis 3° du code des postes et des communications électroniques
8 Il s'agit de celles listées à l'article R. 10-13 V du code des postes et des communications électroniques
9 Article L. 34-1 III du code des postes et des communications électroniques
10 Cons. const. 18 janvier 1995, n°94-352 DC ; Cons. const. 23 juillet 1999, n°99-416 DC
11 Cons. const. 16 juillet 1996, n°96-377 DC
12 CJUE, grande ch., Digital Rights Ireland, 8 avril 2014, C-293/12 et C-594/12 ; CJUE, grande ch., Tele2 Sverige et a., 21 décembre 2016, C-203/15 et C-698/15 ; CJUE, grande ch. La Quadrature du Net et a., 6 octobre 2020, C-511/18, C-512/18 et C-520/18
13 M. 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 ?*, Veille juridique du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale, n°91, novembre 2020, pp. 13-29
14 B. Nicaud, *CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données*, AJ Pénal 2020, p. 531

I. La nécessité d'une conservation généralisée et indifférenciée des données de connexion aux fins de lutter contre la délinquance

Dans ses arrêts, la CJUE a posé clairement l'interdiction pour les États membres de prévoir des mesures législatives prévoyant à titre préventif une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales[15].
En revanche, la CJUE a admis la possibilité de prévoir une telle conservation dans des situations où un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible[16].

De même, dans son arrêt Quadrature du Net, la CJUE admet l'hypothèse de la conservation ciblée, en amont, des données en fonction de zones géographiques prédéfinies pour des infractions relevant de la « criminalité grave ». Elle envisage également d'hypothèse d'une conservation rapide des données permise par le droit européen[17].

Toutefois, comme l'a relevé le Conseil d'État, la solution suggérée par la CJUE de mettre en œuvre cette conservation ciblée des données de connexion n'est ni matériellement possible, ni opérationnellement efficace[18]. En effet, il n'est tout simplement pas possible de prédéterminer les personnes qui seront impliquées ultérieurement dans une infraction pénale qui n'a pas encore été commise. Le raisonnement est identique s'agissant du lieu de commission de cette infraction[19].

Saisissant cette infaisabilité opérationnelle, le Conseil d'État suggère de recourir à la conservation rapide autorisée par le droit européen en s'appuyant sur le stock de données conservées de façon généralisée et indifférenciée pour les besoins de la sécurité nationale. Ce stock peut ainsi être utilisée pour la poursuite des infractions pénales[20]. Autrement dit, le critère lié à la sécurité nationale devient le support juridique autorisant l'accès judiciaire à ces données sous deux réserves : la lutte contre la criminalité grave et une autorisation préalable délivrée par une autorité administrative indépendante ou un juge indépendant ayant la qualité d'un tiers par rapport aux enquêteurs.

---

15 CJUE, grande ch., Digital Rights Ireland, 8 avril 2014, C-293/12 et C-594/12 ; CJUE, grande ch., Tele2 Sverige et a., 21 décembre 2016, C-203/15 et C-698/15 ; CJUE, grande ch. La Quadrature du Net et a., 6 octobre 2020, C-511/18, C-512/18 et C-520/18
16 CJUE, grande ch. La Quadrature du Net et a., c-511/18, c-512/18 et C-520/18, §139,168
17 Articles 16 et 17 de la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001
18 CE, Ass., French Data Network, 21 avril 2021, point 54
19 M. Audibert, Conservation des métadonnées : le Conseil d'État préserve la majorité des enquêtes judiciaires, Lexbase Pénal, n°38, 20 mai 2021, pp. 85-87
20 CE, Ass., French Data Network, 21 avril 2021, point 57

Ce dialogue complexe, sinon « rugueux »[21], des juges[22] et la position d'équilibre du Conseil d'État traduit l'immense enjeu que représente la conservation généralisée et indifférenciée des données de connexion. Récemment, le Conseil constitutionnel a été amené à se prononcer sur la constitutionnalité de l'ancien régime juridique de conservation des données[23]. Dans une décision du 25 février 2022[24], le Conseil constitutionnel a déclaré contraire à la Constitution cet ancien régime juridique dans la mesure où la conservation générale et indifférenciée des données de connexion portent une atteinte disproportionnée au droit au respect de la vie privée[25].

Constatant d'une part que ces dispositions ne sont plus en vigueur et d'autre part que la remise en cause des mesures ayant été prises sur le fondement de ces dispositions déclarées contraires à la Constitution méconnaîtrait les objectifs de valeur constitutionnelle de sauvegarde de l'ordre et de recherche des auteurs d'infractions et aurait dès lors des conséquences manifestement excessives, le Conseil énonce que ces mesures ne peuvent être contestées sur le fondement de cette inconstitutionnalité[26]. Si des interrogations subsistent concernant le régime actuel de conservation des données et les procédures en cours[27], il n'en demeure pas moins que le Conseil constate que cette conservation des données de connexion revêt un intérêt majeur.

En effet, d'un point de vue opérationnel, cette question est centrale. Les données de connexion sont massivement utilisées dans le cadre des enquêtes ou des informations judiciaires[28]. En pratique, il s'agit des réquisitions visant à obtenir des informations permettant l'identification d'un utilisateur, des données relatives aux équipements terminaux de communications utilisées, les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication[29], etc.

En 2020, plus de 85% des enquêtes s'appuyaient sur ces données de connexion[30]. En volume, cela représente environ 2,5 millions de réquisitions judiciaires adressées aux opérateurs de communications électroniques[31]. Ces données permettent d'identifier l'auteur d'un cyberharcèlement, d'un revenge porn, de reconstituer le parcours d'un individu suspecté de meurtre, de croiser ses données téléphoniques avec celles de la victime pour pouvoir lui imputer les faits. Elles permettent également d'identifier ceux qui diffusent des contenus illicites sur Internet tels les contenus pédopornographiques, l'apologie du terrorisme. Elles

---

21 N. Hervieu, *Dialogue « rugueux »*, Gazette du Palais, n°34, 5 octobre 2021, p. 3

22 M. Lassale, *Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE*, Recueil Dalloz, 2021, p. 406

23 Article L. 34-1 du code des postes et des communications électroniques en vigueur jusqu'au 31 juillet 2021 et issu de la loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

24 Conseil const. 25 février 2022, n°2021-976/977 QPC

25 Ibid. cons. 13

26 Ibid. cons. 16 et 17

27 Au titre du principe de primauté du droit de l'Union sur le droit national

28 Articles 60-1,60-2, 77-1-1, 77-1-2, 99-3 et 99-4 du code de procédure pénale

29 Article A. 43-9 du code de procédure pénale

30 Alice Vitard, *Pourquoi la France entame-t-elle un bras de fer avec l'Europe sur la conservation des métadonnées ?,* L'Usine Digitale, 26 mars 2021

31 Vie publique, *Données de connexion : leur conservation jugée conforme au droit européen,* 28 avril 2021

sont enfin indispensables pour identifier les co-auteurs ou complices d'une atteinte aux biens ou leurs éventuels receleurs.

Fort de ces constats, maintenir la conservation des données de connexion apparait primordial. Toutefois, considérant la nécessité de maintenir un équilibre permanent entre le droit au respect de la vie privée et la nécessité de poursuivre les auteurs d'infractions, il apparait nécessaire de redéfinir les modalités d'accès à ces mêmes données.

II. Vers une redéfinition de l'accès aux données de connexion afin de concilier le droit au respect de la vie privée et la nécessité de poursuivre les auteurs d'infractions

Cet accès par les autorités publiques aux données de connexion revêt nécessairement une sensibilité particulière puisque, comme cela a été démontré, celles-ci permettent de révéler les usages numériques d'un utilisateur ou encore de reconstituer a posteriori un parcours par le biais des données de localisation.

Le Conseil constitutionnel comme la CJUE ont apporté des précisions sur les modalités de cet accès s'agissant du contrôle de proportionnalité dans l'atteinte au droit au respect de la vie privée.

Dans une décision récente, le Conseil constitutionnel a jugé inconstitutionnel, dans le cadre de l'enquête préliminaire, la réquisition des données de connexion par le procureur de la République ou, sur autorisation de celui-ci, par l'officier ou l'agent de police judiciaire[32]. Examinant les garanties qui entourent cet accès, le Conseil constate qu'il y a une garantie procédurale constituée par l'autorisation donnée par le procureur de la République, magistrat de l'ordre judiciaire, mais qu'elle est la seule, cette seule garantie étant alors insuffisante. Ainsi, il ne remet pas en cause, en soi, l'accès aux données de connexion. Il exige en revanche d'autres garanties procédurales que le législateur doit prévoir considérant l'ingérence dans le droit au respect de la vie privée.

Considérant les enjeux immenses d'une abrogation immédiate, le Conseil a reporté au 31 décembre 2022 l'abrogation des dispositions contestées. Ce report d'une durée supérieure à un an implique que le législateur prenne la mesure des modifications substantielles de la procédure pénale à réaliser. Suivant les options implicitement présentées par le Conseil, le législateur pourrait limiter le champ d'application de cet accès à une typologie d'infractions, prévoir une autorisation limitée dans le temps du procureur de la République assortie d'une intervention du juge des libertés et de la détention au-delà d'un certain délai[33].

Tirant les conséquences de la décision du Conseil constitutionnel, le législateur a d'ores et déjà modifié les dispositions du code de procédure pénale afin d'encadrer et de limiter le recours aux réquisitions visant à obtenir des données de connexion. Ainsi, la loi n°2022-299 du 2 mars 2022 visant à combattre le harcèlement prévoit un nouvel article 60-1-2 du code de procédure pénale. Les réquisitions portant sur les données de connexion ne seront possibles, à peine de nullité, si les nécessités de la procédure l'exigent que dans les hypothèses suivantes : « la

32 Cons. const. 3 décembre 2021, n°2021-952 QPC

33 M. Audibert, *Inconstitutionnalité différée des réquisitions de données informatiques par le procureur de la République dans le cadre de l'enquête préliminaire : le jour d'après*, Lexbase Pénal, n°44, 23 décembre 2021

procédure porte sur un crime ou sur un délit puni d'une peine de trois ans d'emprisonnement ; la procédure porte sur un délit puni d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques et ces réquisitions ont pour seul objet d'identifier l'auteur de l'infraction ; ces réquisitions concernent les équipements terminaux de la victime et interviennent à la demande de celle-ci en cas de délit puni d'une peine d'emprisonnement ; ces réquisitions tendent à retrouver une personne disparue dans le cadre des procédures prévues aux articles 74-1 ou 80-4 du code de procédure pénale ou sont effectuées dans le cadre de la procédure prévue à l'article 706-106-4 »[34]. Nous avons donc ici des conditions supplémentaires prévues par le législateur et uniquement liées au périmètre infractionnel sur le critère de la gravité de la sanction pénale avec une disposition spécifique lorsqu'un réseau de communications électroniques a été utilisé par l'auteur de l'infraction.

Toutefois, si le Conseil constitutionnel a demandé des garanties supplémentaires, il convient de noter que la CJUE a d'ores et déjà adopté une position plus tranchée.

Dans un arrêt du 2 mars 2021[35], la Cour déclare que le droit de l'Union européenne s'oppose à une législation nationale donnant compétence au ministère public, qui dirige l'enquête judiciaire et exerce, le cas échéant, l'action publique, pour autoriser l'accès par les enquêteurs aux données de connexion. Celle-ci explique en substance que l'autorité qui exerce le contrôle de proportionnalité préalable ne peut être la même que celle qui sollicite l'accès aux données de connexion[36]. Cette autorité ne doit pas être impliquée dans la conduite de l'enquête pénale.

Si le procureur de la République semble d'emblée exclu de cette faculté, par ricochet et dans la mesure où le juge d'instruction dirige l'information judiciaire[37] et peut requérir la communication de données de connexion[38], celui-ci voit cette prérogative directement remise en cause par la CJUE.

Ainsi, au travers de l'enjeu relatif à l'accès aux données de connexion, nous sommes en droit de nous interroger sur le fait de savoir si nous ne sommes pas à l'aune d'un basculement majeur de notre procédure pénale. Ce basculement pourrait consister en la création d'un juge de l'enquête : magistrat non impliqué dans la procédure et qui serait uniquement chargé, à la demande des enquêteurs, du procureur de la République ou du juge d'instruction, d'autoriser certains actes attentatoires à des droits et des libertés.

Ce basculement soulèverait de nombreuses questions capacitaires en matière d'absorption du volume de réquisitions et s'agissant de la nécessité de traiter rapidement les demandes émises par les enquêteurs, eu égard au risque de déperdition des preuves.

---

[34] Article 60-1-2 du code de procédure pénale

35 CJUE, Prokuratuur, 2 mars 2021, C-746/18

36 M. Audibert, *La conservation et l'accès aux métadonnées dans le cadre des enquêtes judiciaires : vers un bouleversement dans la procédure pénale française ?,* Lexbase Pénal, n°36, 25 mars 2021, pp. 73-78

37 Article 81 du code de procédure pénale

38 Article 99-3 du code de procédure pénale

Biographie

Officier de gendarmerie, le chef d'escadron Matthieu Audibert est juriste de formation, spécialisé en droit pénal et en procédure pénale appliqués à la cybercriminalité.
Diplômé de l'université Paris Nanterre, de Sciences Po Aix en Provence, de l'université de Montpellier et de l'École des officiers de la gendarmerie nationale, il est affecté au commandement de la gendarmerie dans le cyberespace. Il dirige le département partenariats et coopération au sein de la division Stratégie, Prospective et Partenariats.
Il prépare une thèse de doctorat en droit privé et sciences criminelles portant sur le recueil de la preuve numérique en procédure pénale.