# Conservation et accès aux données de connexion : le grand écart entre sécurité et libertés !

C'est un sujet à rebondissements multiples ! Entre textes et jurisprudence sur la conservation des données de connexion, opérateurs télécoms, hébergeurs et fournisseurs en ligne sont ballotés. Mais il y a une constante : pas de conservation généralisée et indifférenciée, et l'accès y est limité.

Par Christiane Féral-Schuhl*, avocate associée, cabinet Féral

Rappelons tout d'abord que les données de connexion désignent les informations techniques qui sont automatiquement engendrées par les communications effectuées *via* Internet ou par téléphonie. Il s'agit en quelque sorte des informations qui « enveloppent » un message, par exemple le nom et l'adresse IP d'un internaute, l'heure et la durée d'un appel téléphonique... Ce sont elles qui vont permettre de géolocaliser une conversation, ou de déterminer que telle personne échangeait à telle heure avec telle autre, ou encore qu'elle lui a transmis un message de tel volume.

## Pas de conservation généralisée

On imagine donc assez aisément l'intérêt que peuvent avoir la collecte et l'utilisation de telles données et les atteintes que cela peut porter au droit fondamental à la confidentialité des communications. C'est précisément pour préserver le droit au respect de la vie privée que la conservation des données de connexion est interdite par principe. Les opérateurs télécoms, les fournisseurs d'accès à Internet ou encore les hébergeurs doivent donc effacer ou rendre anonymes les données relatives aux communications électroniques. Et ce, conformément à l'article 34-1 du code des postes et des communications électroniques (CPCE). Mais il existe des exceptions, envisagées immédiatement par le même texte, notamment pour prévenir les menaces contre la sécurité publique et la sauvegarde de la sécurité nationale, ainsi que pour lutter contre la criminalité et la délinquance grave. Aussi, les opérateurs de communications électroniques doivent-ils conserver un certain temps – pour des raisons tenant à la défense d'intérêts publics ou privés – les données de connexion.

Ces obligations pèsent ainsi sur les fournisseurs d'accès – au cloud notamment – et d'hébergement mais aussi sur les entreprises qui fournissent un accès Wifi au public à partir d'une connexion Internet, en ce qu'elles sont assimilées à un intermédiaire technique. C'est ce que précise le même article 34-1 du CPCE : *« Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions* [sur la conservation des données de connexion, ndlr] ». Ces acteurs se trouvent donc au cœur d'un arsenal sécuritaire avec des obligations qui n'en finissent pas de fluctuer au gré des réponses apportées par le législateur et/ou par le juge, tant au niveau national qu'européen.

La Cour de justice de l'Union européenne (CJUE) rappelle, de manière constante (1) que la conservation généralisée et indifférenciée, à titre préventif, des données de connexion par les opérateurs est interdite. Cependant, elle admet qu'une restriction au droit à la vie privée est possible lorsqu'elle est justifiée par une nécessité urgente, pour une durée déterminée, et lorsqu'elle constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique. Autrement dit, la haute juridiction européenne autorise l'obligation de conservation « ciblée » des données, obligation qui peut être renouvelable en cas de persistance de la menace.

C'est également la position adoptée par la CJUE qui s'est exprimée sur le sujet à deux reprises en 2022 : en avril d'abord, concernant la localisation d'appel téléphonique obtenue sur le fondement d'une loi irlandaise (2); en septembre 2022 ensuite, cette fois pour des poursuites pénales de délits d'initiés engagées sur le fondement du décret français de lutte contre les infractions d'abus de marché (3). Dans les deux cas, la haute juridiction européenne confirme que les législations nationales des Etats membres ne peuvent aboutir à la conservation généralisée et indifférenciée des données de trafic. A défaut, elle les juge contraire au droit de l'Union européenne.

## En France, 3 décrets : délais de 1 à 5 ans

En France, la mise en œuvre de ce dispositif a donné lieu à l'entrée en vigueur de différentes obligations, répondant à un certain nombre de cas limitativement énumérés et pour une durée qui varie d'un an à cinq ans selon les informations concernées. Ces obligations sont prévues par trois décrets pris en application de l'article L.34-1 du CPCE, encore lui. Leur périmètre est en constante évolution, à la recherche d'un équilibre entre objectifs sécuritaires et protection de la vie privée :

### Notes

(1) - Arrêts « Digital Rights » en 2014, « Télé 2 » en 2016, et encore trois autres arrêts en 2020.

(2) - CJUE, affaire C140/20, arrêt du 05-04-22.

(3) - CJUE, affaires jointes C-339/20 et C-397/20, arrêt du 20-09-22.

(4) - Le décret n°2021-1362 abroge et remplace le décret n°2011-219 du 25-02-11.

• Le décret n°2021-1361 relatif aux catégories de données conservées par les opérateurs de communications électroniques.
• Le décret n°2021-1362 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (4).
• Le décret n°2022-1327 portant injonction, au regard de la menace grave et actuelle contre la sécurité? nationale, de conservation pour une dure?e d'un an de certaines catégories de données de connexion (5).

## Cour de cassation : les arrêts de l'été 2022

Quant à nos juridictions nationales, elles se sont penchées plus spécifiquement sur la question des personnes habilitées à avoir accès à ces données. Le législateur français a prévu que seules l'autorité judiciaire et certaines administrations – par exemple, les services de renseignement – peuvent exiger la communication des données de connexion. Le Conseil constitutionnel, saisi d'une question prioritaire de constitutionnalité (QPC) à l'initiative d'associations de défense des droits et libertés sur Internet (6), a considéré que les agents des douanes étaient exclus de ce périmètre. Ils ne peuvent donc pas exiger la communication de ces données (7).

La Cour de cassation a, quant à elle, apporté quelques précisions complémentaires dans plusieurs arrêts rendus au cours de l'été 2022, en juillet (8). Elle considère que l'accès aux données de connexion doit se faire sous le contrôle effectif d'une juridiction. En conséquence, le juge d'instruction – qu'elle a qualifié de juridiction indépendante et non de partie – ou une autorité administrative indépendante peuvent ordonner et contrôler les procédures d'accès aux données de connexion. En revanche, le procureur de la République, parce qu'il est une autorité de poursuite et non une juridiction, ne dispose pas de cette possibilité. En conséquence, l'accès aux données de connexion, lorsqu'il est ordonné par un procureur, serait irrégulier. De quoi remettre en cause la régularité de beaucoup de procédures pénales !

La haute juridiction française, dans ces mêmes arrêts du mois de juillet, a rappelé que la personne mise en examen, victime d'un accès irrégulier, a la possibilité de contester la pertinence des preuves tirées de ses données. De quoi permettre au juge pénal d'annuler les actes ayant permis d'accéder aux données !

La Conférence nationale des procureurs de la République (CNPR) y voit un *« obstacle majeur à l'identification des délinquants et criminels »*, et a dénoncé les *« conséquences* [de ces décisions] *sur la capacité des magistrats du ministère public et des enquêteurs à exercer leurs missions de manifestation de la vérité et de protection des victimes »*. En dépit de cette levée de boucliers, la chambre criminelle de la Cour de cassation a entériné fin octobre 2022 (9) son analyse. Elle confirme que le juge d'instruction, qui est une juridiction, doit contrôler le respect par les enquêteurs des modalités d'accès aux données de trafic et de localisation qu'il a autorisées. Or, dans l'affaire en question, le magistrat instructeur n'avait pas autorisé en des termes spécifiques de sa commission rogatoire les réquisitions litigieuses, et ce notamment parce qu'il n'avait pas précisé la durée et le périmètre de cette commission rogatoire. La Cour de cassation a donc jugé que des réquisitions adressées aux opérateurs télécoms par les enquêteurs devaient être annulées sous réserve qu'un grief soit établi par le requérant.

La haute juridiction a précisé, dans ce même arrêt, que la preuve de ce grief suppose la démonstration de trois éléments : l'accès a porté sur des données irrégulièrement conservées ; la finalité ayant motivé l'accès aux données doit être moins grave que celle ayant justifié leur conservation (hors hypothèse de la conservation rapide) ; l'accès a dépassé les limites de ce qui était strictement nécessaire.

Le sujet a pris une dimension politique, en écho aux magistrats du Parquet. Deux sénateurs (LR) ont considéré que ces décisions *« [les] privent ainsi que les forces de police judiciaire d'un outil précieux dans l'identification des auteurs de crimes ou d'infractions graves »*. Yves Bouloux (10) et Serge Babary (11) ont chacun saisi le gouvernement d'une question écrite (12) afin que ce dernier prenne en urgence les mesures nécessaires afin de permettre aux procureurs de la République d'exercer leurs missions. Serge Babary a même appelé à envisager une réforme institutionnelle afin de conférer aux magistrats du Parquet les garanties d'indépendance exigées par le droit de l'Union européenne.

## Les défenseurs de la vie privée veillent

Mais la question est loin de faire consensus avec ceux qui dénoncent avec force les *« velléités sécuritaires du gouvernement »*. En première ligne de ces défenseurs de la vie privée, il y a notamment l'association La Quadrature du Net, qui salue comme autant de bonnes nouvelles les décisions qui diminuent l'obligation de conservation des données de connexion. Ce fut le cas notamment en février 2022 à la suite de la décision du Conseil constitutionnel qui avait censuré une partie de l'obligation de conservation généralisée et indifférenciée des données de connexion. (13)

Si la lutte contre la criminalité légitime l'ingérence de l'Etat, reste donc toujours et encore à positionner le curseur à bon niveau pour ne pas porter atteinte à la vie privée et aux libertés individuelles. @

* Christiane Féral-Schuhl, ancienne présidente du Conseil national des barreaux (CNB) après avoir été bâtonnier du Barreau de Paris, est l'auteure de *« Cyberdroit »* (Dalloz 2019-2020) et co-auteure de *« Cybersécurité, mode d'emploi »* (PUF 2022).

### Notes

**(5)** - Le décret n°2022-1327 prolonge pour un an l'obligation qui était prévue par le décret n°2021-1363.

**(6)** - Dont La Quadrature du Net.

**(7)** - https://lc.cx/CC-QPC-15-02-19

**(8)** - Cour de cassation, chambre criminelle, arrêts du 12-07-22, pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652.

**(9)** - Cour de cassation, chambre criminelle, 25-10-22, pourvoi n° 21-87.397.

**(10)** - https://lc.cx/QuestionYB

**(11)** - https://lc.cx/QuestionSB

**(12)** - Questions écrites à l'attention du garde des sceaux (ministre de la Justice).

**(13)** - https://lc.cx/LQDN-Victoire 25-02-22