Nous n'avons volontairement pas corrigé les imperfections de forme qui peuvent apparaître dans chaque copie.

Concours interne

1ère épreuve d'admissibilité : Droit public

Meilleure copie **Note : 15,5/20**

Ministère de l'intérieur

Direction des libertés publiques
et des affaires juridiques

Lundi 26 août 2019

Note au directeur

Objet : Le traitement des données de connexion dans le cadre des missions relevant de la sécurité intérieure

_____

Les données de connexion constituent désormais un élément indispensable dans la lutte contre la criminalité organisée, le terrorisme et de façon générale toutes les menaces pesant sur la sécurité intérieure.

Les données de connexion regroupant l'ensemble des informations ou documents traités ou conservés par les réseaux et services de communications électroniques des opérateurs de communications électroniques et de services numériques. Communément identifiées sous le terme des données personnelles, la collecte et le traitement de ces données relèvent à la fois d'un enjeu économique à l'importance croissante et d'un impératif de sécurité intérieure incontournable.

La conciliation de ces impératifs, sécuritaire et économique, avec la protection des libertés fondamentales, notamment le droit au respect de la vie privée, demande un cadre juridique efficace et adapté.

Face aux risques sécuritaires, notamment liés au terrorisme, de nombreux textes législatifs et réglementaires ont considérablement augmenté les capacités d'accès à ces données par les services chargés de la sécurité intérieure. Parallèlement, d'abord au niveau national puis au niveau européen, un cadre réglementaire stricte a été mis en place pour contrôler l'usage et la collecte de ces données par les opérateurs économiques. Ainsi, le règlement général sur la protection des données adopté en 2016 et entré en vigueur en 2018 a renforcé les garanties offertes aux citoyens quant au traitement de leurs données personnelles.
La conciliation des droits fondamentaux avec l'impératif de sécurité intérieure présente un défi particulier tenant à l'importance du débat public qui entoure les données de connexions et leurs usages. De récentes décisions,

notamment de la Cour de justice de l'Union européenne (CJUE), suggèrent qu'il serait utile de faire évoluer le cadre juridique actuel pour renforcer l'efficacité et la sécurité juridique du dispositif.

Pour en permettre l'accès par les services chargés de la sécurité intérieure, le droit français suppose un traitement et la conservation d'un nombre important de données de connexion, notamment par les opérateurs économiques (I). Un renforcement des garanties relations aux droits fondamentaux apparait necessaire pour adapter le dispositif actuel et en assurer la sécurité juridique (II).

I) Le traitement et la conservation des données de connexions sont nécessaires afin de permettre aux services chargés de la sécurité intérieure d'assurer pleinement leurs missions

A) Une capacité d'accès aux données de connexion détenues par les opérateurs permettant de répondre aux enjeux contemporains relatifs à la sécurité intérieure

La place grandissante que prennent les technologies numériques, tant dans la vie courante que pour la réalisation d'infractions graves ou d'actes de terrorisme, supposent que les données que ces technologies collectent à des fins commerciales soient accessibles aux agents chargés de missions de sécurité publique.

Aujourd'hui, le Code de la sécurité intérieure permet trois formes d'accès aux données de connexions. D'une part, la réquisition administrative prévue à l'article L.851-1, d'autre part, les demandes d'accès en temps réel prévues par les L.851-2 et L.851-4. Enfin, l'article L.851-3 du même code permet de recueillir, par un traitement automatisé, des données en lien avec une menace terroriste.

L'article L.851-1 dispose que les données concernées sont « des informations ou documents traités ou conservés », par les réseaux ou services de communications électroniques des opérateurs, « y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques des opérateurs, « y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications (…) », sont exclu le contenus des communications. Les données font l'objet d'une demande d'accès par des agents habilités, la demande doit être motivée et soumise à la décision d'une personne désignée par la Commission nationale de contrôle des techniques de renseignement et placée auprès du Premier ministre. La demande d'accès aux données en temps réel fait-elle l'objet d'une autorisation écrite au Premier ministre et d'un contrôle du président de la Commission nationale de contrôle des techniques de renseignement.

B) Une obligation de traitement et de conservations des données de connexion rendue nécessaire par les besoins d'accès des services chargés de la sécurité intérieure.

Les articles précités du Code de la sécurité intérieure n'imposent pas formellement la conservation des dossiers de connexion ou un retraitement par les opérateurs. Néanmoins, comme l'a souligné le Conseil d'Etat, cette obligation est induite par les dispositions.

La nature des données ciblées, qui sont très largement définies, impose nécessairement aux opérateurs de traiter, d'organiser et de conserver ces données. L'article L.851-3 impose lui un traitement automatisé des données sur les réseaux des opérateurs, afin de dégager celles relatives aux menaces terroristes.

Le législateur avait bien conscience de cette obligation induite, prévoyant à la suite de ces dispositions un mécanisme indemnitaire visant à couvrir les surcoûts des opérateurs.

Il convient cependant de souligner que les opérateurs de communications électroniques et les opérateurs de services numériques génèrent et collectent ces données de façon régulière pour les besoins et le suivi de leurs activités économiques, indépendamment des besoins de la sécurité intérieure. Néanmoins, si ce traitement commerciale des données de connexion fait l'objet d'un contrôle (récemment renforcé par l'adoption du « RGPD » en 2016) afin de prévenir des atteintes trop importantes aux libertés publiques, ce contrôle est plus limité s'agissant de traitement des données de connexions pour les besoins de la sécurité intérieure.

_____

II) Le contrôle du traitement des données de connexion, nécessaire pour la sécurité intérieure, doit-être renforcé pour assurer l'efficacité et la sécurité juridique du dispositif.

A) Un contrôle existant, mais limité face à l'impératif de sécurité intérieure, aujourd'hui remis en cause.

Le contrôle de l'accès aux données de connexions est actuellement réalisé par le Premier ministre et par la Commission nationale de contrôle des techniques de renseignement. Le Conseil d'Etat joue également un rôle, pouvant être saisi par toute personne souhaitant vérifier qu'aucune technique n'est irrégulièrement mise en œuvre ou par le président de la Commission nationale de contrôle des techniques de renseignement si le Premier ministre ne donne pas suite aux avis de la Commission, ou que ces suites sont insuffisantes.

Cependant, d'une part la procédure n'est pas contradictoire, ce qui s'explique par le fait que les éléments en cause sont couverts par le secret de la défense nationale, d'autre part les personnes qui ont pu être victime d'une demande d'accès ou d'un accès irrégulier à des données de connexion ne sont pas informées. Ces exceptions aux libertés publiques sont rendues nécessaires pour protéger la sureté de l'Etat.

L'efficacité de la réponse sécuritaire aux menaces, notamment terroriste, impose des mesures d'exceptions qui ont été largement adopté par nos voisins européen. C'est ainsi que la Cour de justice de l'Union Européenne a eu à se prononcé sur un régime juridique proche du régime français et est venue rappeler que le respect du droit à la vie privé, s'agissant des données de connexions, était garanti par le droit européen et que les atteintes qui y sont portées pour les besoins de la sécurité publique devaient être limitées.

La CJUE, dans son arrêt du 21 décembre 2016 « Tele2Sverige » a en effet estimé que le droit suédois, imposant une conservation généralisée et indifférenciée des données de connexions par les opérateurs afin d'en permettre l'accès par les services de sécurité était contraire au droit de l'Union, plus particulièrement la directive 2002/58 relative au traitement des données à caractère personnel et la charte des droits fondamentaux de l'UE. Cette décision, diversement appréciée par les Etats membres, à conduit le Conseil d'Etat à interroger la Cour sur la conformité du droit français au droit européen (CE, 26 juillet 2018).

La conciliation entre les obligations relatives à la sécurité nationale, découlant notamment du droit à la sureté garanti par l'article 6 de la Charte des droits fondamentaux de l'UE, et la protection de la vie privée et des données personnelles demande des améliorations du dispositif. Noton néanmoins que le Conseil Constitutionnel a estimé que les dispositions françaises étaient conformes à la Constitutions et garantissaient le respect des droits avec les objectifs de la sécurité publique (DC 2015 -478 du 24 juillet 2015).

B) Des améliorations peuvent être apportées au dispositif actuel pour assurer un meilleur contrôle de la proportionnalité des données collectées au regard des objectifs de la sécurité intérieure.

Comme le soulignait la Commission nationale de l'informatique et des libertés dans son avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme du 11 juillet 2017 : « [] des mesures de sécurité plus intrusives doit nécessairement s'accompagner des garanties qui encadrent l'action de services de sécurité […] ».

Le dispositif actuel prévoit une autorisation préalable et un controle du Premier ministre, de la Commission nationale de contrôle des techniques de renseignement et du Conseil d'Etat. Cependant, il pourrait être possible de proposer les évolutions suivantes :

1. Prévoir une évaluation tout les cinq ans des fichiers de collectes des données détenus par les services de sécurité afin d'expurger les données personnelles y figurant qui ne s'avéreraient plus nécessaire. Ce contrôle serait réalisé par la Commission nationale du contrôle des techniques de renseignement (CNCTR)

2. Prévoir l'établissement d'un contrôleur des données de connexions, désignés alternativement parmis les membres du Conseil d'Etat et de la Cour de Cassation chargé d'autoriser les demandes d'accès, en lieu et place de la personne qualifiée placée auprès du Premier ministre. La CNCTR conservera sont rôle consultatif et le Premier ministre son autorisation, finale, pour les demandes d'accès en temps réel.

3. Initier, avec les services dépendant du ministère de l'intérieur et les autres services de sécurité, sous l'égide du conducteur national du renseignement une réflexion sur les données de connexions utiles afin de limiter le nombre de données collectives.