FONDATION ROBERT SCHUMAN

POLICY PAPER

Question d'Europe
n°510
8 avril 2019

François MOLINS

"La protection des citoyens européens dans un monde ultra-connecté"

Le 3 avril, la Fondation Robert Schuman organisait à Luxembourg avec l'Institut Max Planck une conférence sur le thème: "La protection des citoyens européens dans un monde ultra-connecté". Y assistaient d'éminentes personnalités représentant les institutions européennes et notamment l'avocat général, Henrik Saugmandsgaard Øe, représentant le Président de la Cour de Justice de l'Union européenne.

Un compte-rendu complet de ces travaux sera publié ultérieurement. D'ores et déjà, nous donnons connaissance de la très intéressante communication faite par M. François Molins, Procureur général près la Cour de Cassation de la République française, ancien Procureur près le Tribunal de grande instance de Paris et, à ce titre, en charge de la lutte anti-terroriste. Il alerte notamment sur les besoins des services en charge de la lutte contre le terrorisme et la grande criminalité, quant à la conservation et l'accès aux données électroniques.

Les développements qui suivent sont le fruit de l'expérience qui a été la mienne pendant 7 ans à la tête du parquet de Paris compétent en matière d'antiterrorisme et de lutte contre la criminalité organisée.

Dans ces deux domaines, nous devons tenir compte de plusieurs phénomènes qui constituent autant d'enjeux majeurs:

- En matière terroriste la menace est aujourd'hui durable et endogène. Elle est le fait d'individus, présentant souvent des signaux faibles et qui, adhérents aux thèses mortifères de Daech et n'ayant pu rejoindre la zone irako-syrienne, peuvent être tentés ou inspirés de passer individuellement à l'acte conformément aux mots d'ordre permanents de cette organisation terroriste. Cette menace est diffuse et donc d'autant plus difficile à détecter pour les services de renseignement des Etats.
- En matière de criminalité organisée, les organisations criminelles se professionnalisent de plus en plus et leurs chefs n'ont plus besoin d'aller sur le terrain pour donner leurs directives. Ils utilisent les nouvelles technologies. La direction des opérations criminelles est de plus en plus souvent dématérialisée et protégée par des procédés de cryptage.
- Enfin les moyens de preuve ont considérablement évolué. La preuve électronique résultant des données de connexion et de localisation ainsi que les données de contenu des échanges électroniques prennent une part de plus en plus importante dans les enquêtes judiciaires et devant les juridictions pénales.

A l'aune de ces réflexions, j'évoquerai essentiellement la problématique de la conservation des données de trafic et de localisation et les conséquences de l'actuelle jurisprudence de la Cour de justice de l'Union Européenne.

Les données de connexion également appelées "métadonnées" ou données relatives au trafic et données de localisation portent, non pas sur le contenu des messages, mais sur les conditions dans lesquelles ces derniers ont été consultés ou échangés. Elles sont donc relatives à l'identité et à la localisation del'auteur et du destinataire de communications, à la date et à la durée de celles-ci, aux matériels, numéros de téléphone et adresses IP utilisés. L'exploitation de ces données repose sur leur conservation généralisée, indifférenciée, pendant un certain temps par les opérateurs de communications électroniques, qui sont tenus d'y procéder par la loi. Elle 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 (géolocalisation).

Il s'agit donc pour l'Etat, d'une arme très précieuse, notamment dans la lutte contre la menace terroriste contemporaine dont on connaît le caractère massif ou diffus.

C'est une évidence en matière de lutte antiterroriste. En matière de criminalité organisée, cela l'est tout autant car aujourd'hui, les chefs des organisations criminelles ne relèvent plus de modes de surveillance classiques. Ils ne vont plus sur le terrain, ils restent à distance et donnent leurs instructions en utilisant les nouvelles technologies

Le 21 décembre 2016, dans une décision *Télé 2 Sverige et Davis* qui a été très largement commentée sous l'angle d'un renforcement de la protection de la vie privée, la Cour de justice de l'Union européenne a jugé que n'étaient pas conformes au droit de l'Union les législations nationales qui prévoyaient *une conservation généralisée et indifférenciée de l'ensemble des données de trafic et de localisation* et qui n'encadraient pas suffisamment leur consultation par les autorités nationales. La Haute Juridiction retient ainsi que si la conservation des données est possible, elle doit être ciblée et limitée au strict nécessaire. La consultation de ces données ne peut être autorisée que par un juge ou une autorité administrative indépendante. Cette décision a été explicitée par un arrêt du 2 octobre 2018 Ministerio fiscal C-207/16.

Ces exigences fragilisent les législations nationales et notamment la législation française en ce qui concerne la conservation et l'accès aux données de connexion, tant pour les services de renseignements qui sont pourtant placés sous le contrôle de la Commission nationale de contrôle du traitement du renseignement que pour les investigations judiciaires placés sous la direction des magistrats.

Ces principes applicables ne sont toutefois pas stabilisés dès lors que plusieurs questions préjudicielles sont pendantes devant le CJUE. Elles ont été posées par le Royaume Uni, par la Cour constitutionnelle belge le 2 août 2018, par le Conseil d'Etat français le 26 juillet 2018, enfin, par la juridiction estonienne le 29 novembre 2018. Par ces questions, les juridictions nationales ont invité la CJUE à préciser notamment, s'il n'yapas lieu de tempérer l'interdiction de la conservation généralisée de données en prenant en compte la gravité de la menace (Conseil d'Etat), et si le procureur peut être regardé comme une Autorité administrative indépendante au sens que la CJUE donne à cette expression (Estonie).

Si cette décision Télé2 venait à être confirmée, l'impact de cette jurisprudence sur les enquêtes en matière de terrorisme et de criminalité organisée ne peut que soulever une vive inquiétude. Il est à craindre que la Cour de Luxembourg n'ait en effet pas maîtrisé comment les services qui sont chargés des investigations parviennent à identifier des auteurs de crimes ou des membres de réseau criminel, dont la parfaite maîtrise des techniques policières les conduit à "professionnaliser" l'effacement des traces et indices traditionnels. La conservation des données et un accès contrôlé mais fluide apparaissent ainsi désormais comme le préalable au succès des investigations en droit commun, en criminalité organisée et bien sûr en terrorisme.

Le sens général de la décision précitée et la lecture que fait la Cour de la directive 2002/58 concernant le traitement des données à caractère personnel paraissent sans ambiguïté: la conservation ne devrait être que très limitée dans son champ infractionnel - uniquement pour la lutte contre la criminalité grave - et dans son champ matériel - limité au strict nécessaire pour les données, les personnes et le temps-.

Le fondement de la décision repose sur les articles 7 (respect de la vie privée et familiale), 8 (protection des données à caractère personnel), 11 (liberté d'expression) et 52 (respect du principe de la proportionnalité dans les atteintes aux droits) de la Charte des droits fondamentaux de l'Union européenne. Il s'agit là du coeur du droit de l'Union et des Etats démocratiques qui la composent.

La capacité de combiner la protection de ces droits et de ceux reconnus aux article 2 (droit à la vie) et 6 (droit à la liberté et à la sûreté) n'est cependant évoquée ni

dans la décision, ni dans la plupart des commentaires qui en sont faits. La Cour de justice semble même accorder un poids relativement faible à l'objectif d'intérêt général de la lutte contre le terrorisme puisque dans le point 103 de l'arrêt télé 2, tout en reconnaissant explicitement l'efficacité de la conservation générale des données, elle estime que cela ne suffit pas à rendre cette mesure nécessaire.

Or ce contrôle de la proportionnalité apparaît comme une question fondamentale qui se pose à notre société. A l'ère numérique, la p otection de la vie privée et des données à caractère personnel est une des garanties essentielles de nos libertés. Mais celle-ci doit-elle 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?

C'est la question que soulève la décision du 26 décembre 2016 de la Cour de justice de l'Union européenne. Si elle était confirmée et que l'interprétation des principes qui y sont ébauchés devait être stricte, la conséquence immédiate serait la fin de nombre des enquêtes pénales qui sont actuellement en cours [voire la nullité des actes déjà réalisés] que celles-ci concernent des faits d'atteintes graves aux personnes de droit commun - homicides, viols -, des infractions relevant de la criminalité organisée ou des actes de terrorisme.

Les conditions que pose la Cour pour avoir accès aux données paraissent peu ancrées dans la réalité. La Cour exige ainsi que "la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées, ainsi que la durée de conservation retenue, limitée au strict nécessaire". La Cour juge que celles-ci peuvent être délimitées selon des critères alternatifs, par référence à un cercle de personnes soupçonnées, à une période temporelle ou encore à une zone géographique.

C'est une vue de l'esprit!

Dans sa mise en oeuvre, cet attendu signifie qu'il n'y a plus de conservation de données utiles.

Par hypothèse, à l'exception 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. La décision *Téle2 Sverige et Davis* de la Cour de justice de l'Union européenne parait dès lors fondée sur un raisonnement qui, s'il est juridiquement compréhensible, est matériellement irréaliste.

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.

Les données de connexion sont essentielles aux enquêtes dans un cadre administratif comme dans un cadre judiciaire. Elles constituent une "matière première" essentielle pour les magistrats et les enquêteurs.

S'agissant des données de téléphonie, les demandes adressées aux opérateurs peuvent être de deux types:

- à partir d'un numéro de téléphone (relevé des appels émis et reçus, localisation des appels de la cible, association avec un ou plusieurs boîtiers, etc...)
- à partir d'un relais téléphonique (relevé de l'ensemble des numéros de téléphone ayant déclenché ce relais dans un créneau horaire donné).

Ces demandes visent notamment:

- à localiser une personne ou reconstituer le parcours d'une personne surveillée
- à déterminer le cercle de relations d'une personne (relations d'un individu surveillé dans un cadre de prévention du terrorisme...)
- à détecter la survenance de déplacements atypiques susceptibles d'éclairer une enquête.

Quelques exemples d'utilisation:

- Contre terrorisme dans les filières irako-syriennes: l'étude des données connexion a permis de mettre à jour des contacts en Turquie et en Syrie et d'identifier les relations ayant joué un rôle logistique dans les départs sur zone. Ce sont autant d'éléments de preuves pour identifier une filière organisée.

- L'interpellation en France de Mehdi NEMOUCHE (assassinats du musée juif à Bruxelles le 24 mai 2014) a conduit les enquêteurs à solliciter en urgence les données de connexion disponibles afin d'identifier, à partir de son environnement, l'existence éventuelle d'un autre projet en France, ainsi que de complices. L'enjeu du point de vue de la sécurité nationale était donc essentiel.

- Attentats de Saint Denis et du Bataclan le 13 novembre 2015. Après la commission de ces attentats, nous disposions de maigres indices. Une image issue du dispositif de vidéo-surveillance faisait apparaître un terroriste qui s'était fait exploser au Stade de France en train de téléphoner avec un téléphone portable à 21 h O1, et un téléphone portable retrouvé par les enquêteurs dans une poubelle située face à l'entrée du Bataclan à Paris. Le bornage effectué à partir du relais téléphonique près du Stade de France a permis de recenser 15 094 appels téléphoniques ayant activé ce relais entre 21 h et 21 h 04. L'analyse de ces communications et le croisement avec le contenu du boîtier du téléphone portable découvert devant le Bataclan a permis de démontrer qu'ils avaient tous les deux activé la même puce téléphonique belge. C'est ce qui a permis l'orientation des investigations judiciaires. Si nous n'avions pu immédiatement accéder à ces données de connexion et de localisation de ces téléphones portables, le cours de i'enquête aurait été considérablement ralenti et l'identification des cellules terroristes en France et en Belgique différée, voire obérée.

- dans le cas du projet d'attentat contre l'église de Villejuif précédé d'un homicide volontaire sur une jeune femme, l'analyse de l'activité sur Internet a permis de déterminer que l'auteur présumé avait reçu ses instructions d'une tierce personne basée à l'étranger.

- Elucidation d'assassinat (affaire Hélène PASTOR à Monaco). Le travail d'analyse considérable effectué à partir de 3,5 millions d'appels téléphoniques a été déterminant dans l'identification des auteurs du crime. Il en va de même pour l'affaire Nordahl LELANDAIS, soupçonné d'être l'auteur d'un homicide volontaire sur une enfant de 10 ans puis sur un caporal de l'armée française.

- Enfin, l'analyse des données de connexion sur Internet est indispensable pour déceler des réseaux pédo pomographiques et confondre ceux qui mettent en ligne des contenus ou en font l'acquisition.

L'obtention de ces "métadonnées" constitue donc une arme précieuse et indispensable dans la lutte contre la grande criminalité et particulièrement la menace terroriste contemporaine. Le système de collecte systématique des "métadonnées" revêt en conséquence une importance déterminante dans la protection de la sécurité nationale. Sans lui, dans un cadre administratif, les services de renseignement seraient privés de tout l'historique et dans un cadre judiciaire, tout dépendrait de la capacité des autorités d'anticiper sur l'identité des personnes dont les données de connexion pourraient être utiles, ce qui est impossible.

Enfin la jurisprudence de la Cour de justice diverge de celle de la Cour européenne de Strasbourg et provoque à ce titre une situation d'insécurité juridique puisque dans ses récents développements, la Cour européenne des droits de l'homme a notamment conclu que l'utilisation d'un régime d'interception massive n'emportait pas en lui même violation de la Convention. (Arrêt CEDH Centrum für Rattsiva c/ Suède du 19 juin 2018 et arrêt Big Brother Watch c/ Royaume Uni du 13 septembre 2018). Il faudrait à tout le moins que les Etats membres soient soumis à des critères convergents d'appréciation de la nécessité et de la proportionnalité technique de surveillance selon que l'ingérence est examinée au regard de la Convention européenne ou de la Charte.

Le choix juridique qui s'impose à nos démocraties ne doit pas être protection de la vie privée versus

arrestation des criminels et des terroristes. Le choix juridique doit être celui de la protection de la vie privée par la garantie d'un accès juridictionnellement encadré aux données conservées. La prévention des atteintes à l'ordre public est en effet nécessaire à la sauvegarde des droits et à l'exercice des libertés de nos concitoyens.

Pour les enquêtes judiciaires, l'autorisation d'accès à des données dont la sensibilité est particulièrement importante doit relever des autorités judiciaires qui dans nos démocraties sont les garantes des libertés individuelles. Les mécanismes juridictionnels existant dans les Etats de l'Union doivent permettre de trouver le cadre indispensable à assurer contrôle et efficacité sans sombrer dans le travers qui rend les enquêtes pénales d'un niveau de complexité juridique qui nuit à leur efficacité.

L'équilibre à trouver est délicat mais une protection caricaturale des données personnelles aura pour conséquence immédiate un affaiblissement des autorités chargées d'identifier et de poursuivre les auteurs de crimes. Dans une démocratie, ce sont l'Etat et ces autorités qui sont chargées de protéger les libertés fondamentales. Ce principe m'apparaît comme la garantie d'un fonctionnement optimal de nos institutions. La Cour européenne des droits de l'Homme a souligné ce principe en jugeant que "l'obligation positive des Etats contractants de garantir la protection de la vie privée implique l'obligation de donner aux autorités judiciaires la possibilité d'accéder à des adresses IP dynamiques et à des données de communication en vue d'identifier une personne privée qui aurait violé le droit d'un autre individu au respect de sa vie privée " (CEDH, arrêt K.U, vs Finland, 02/12/2008, n° 2872/02)

En conclusion il m'apparaît qu'une véritable réflexion doit être engagée au regard de tous ces enjeux et des compétences institutionnelles de chacun pour assurer la conciliation de ces impératifs.

Le dialogue des juges est certainement indispensable pour y parvenir en ayant présent à l'esprit les conclusions prémonitoires du commissaire du gouvernement Bruno GENEVOIX qui rappelait en 1978 que "à l'échelon de la communauté européenne, il ne doit y avoir ni gouvernement des juges, ni guerre des juges. Il doit y avoir place pour le dialogue des juges".

François MOLINS

Procureur général près la Cour de cassation

Retrouvez l'ensemble de nos publications sur notre site :
www.robert-schuman.eu

Directeur de la publication : Pascale JOANNIN