Placer la totalité de la population sous surveillance n'est pas la solution au terrorisme.

Les Exégètes amateurs*

10 juin 2017

Placer la totalité de la population sous surveillance préventive n'est pas admissible dans une société démocratique. Voici la conclusion tirée par la Cour de justice de l'Union européenne, dans deux arrêts (*Digital Rights* en 2014 et *Tele2* en 2016) concernant les « données de connexion ». Pour la cour européenne, ces traces numériques enregistrées dans le sillage des communications électroniques de chacun (géolocalisation, appels téléphoniques, connexions Internet, etc.) révèlent des informations précises et sensibles de la vie des personnes. Leur conservation ne peut donc pas être généralisée et systématique ; elle doit à l'inverse être encadrée et limitée afin de garantir le droit fondamental au respect de la vie privée.

Pourtant, les autorités françaises refusent de se plier au droit européen. Depuis 2006, les opérateurs télécoms sont obligés de conserver les données de connexion de la totalité de leurs utilisateurs en France. Ainsi, une poignée de grandes entreprises conservent un véritable journal de bord de la population française permettant de revenir jusqu'à un an dans le passé, pour le mettre à disposition des autorités françaises (police judiciaire mais aussi services de renseignement, régulateurs et autorités administratives comme Hadopi, etc.).

Pourquoi cette conservation préventive a-t-elle lieu ? Dans un article du Monde du 3 juin 2017, la position de l'État français est ainsi résumée : on ne peut réussir à définir, au préalable, quels individus présenteront à l'avenir une menace grave. *« Il n'y a que dans Minority Report que l'on peut savoir a priori sur qui l'on va enquêter. »* [1]

Derrière ce désir de toute puissance technologique qui relève de la science-fiction dystopique — dont les « boîtes noires » de la Loi Renseignement sont la plus récente illustration — se cache en réalité une véritable paranoïa : si chaque citoyen est une menace potentielle, alors il faut des données sur tout le monde. C'est le renversement d'une logique fondatrice du droit pénal : la suspicion généralisée remplace la présomption d'innocence. Ne pas savoir a priori sur qui l'on enquêtera à l'avenir, voilà ce qui *« va vraiment poser problème »* si l'on en croit le commissaire de l'unité de la police nationale en charge de la cybercriminalité (l'OCLCTIC). [2]

En dépit de ces discours alarmistes, jamais l'utilité d'un régime de conservation généralisée des données de connexion n'a été sérieusement démontrée. Outre ce régime, les enquêteurs disposent en réalité de toujours plus de données et de moyens, à mesure que l'informatisation du monde se poursuit. Quantités d'informations peuvent être obtenues lors de perquisitions, d'enquêtes de terrain, d'interceptions ciblées, etc. Qui plus est, de nombreuses données sont de toute manière conservées par les opérateurs pour

*https://exegetes.eu.org

1. "La lutte contre le terrorisme contrariée par un arrêt européen", *Le Monde*, 3 juin 2017, par Martin Untersinger et Elise Vincent
2. *ibid*

des raisons techniques ou commerciales justifiées.

C'est pourquoi, dans les pays où la protection de la confidentialité des communications électroniques est garantie, l'efficacité des services de police n'est en rien amoindrie. Ainsi, de nombreux États européens se sont départis d'un régime de conservation généralisée des données [3]. Les enquêtes de police y sont-elles si inefficaces qu'une décision similaire ne puisse être prise en France ?

La défense de la conservation généralisées des données ressemble bien plus à une obsession policière — dont la France et le Royaume-Uni sont les fers de lance — qu'à une approche raisonnée. Or, cette obsession policière nous conduit dans une impasse : celle d'une politique sécuritaire qui postule que, pour assurer notre sécurité, les gouvernements doivent tous nous considérer comme des suspects potentiels. Faisant fi des mises en garde de l'histoire, elle légitime l'idée radicalement anti-démocratique que tout individu ou groupe qui refuserait de se soumettre à cette surveillance généralisée et préventive pour se préserver une sphère d'intimité ou de confidentialité serait inévitablement suspect. Il n'est dès lors guère surprenant de voir qu'au niveau européen, les gouvernements britannique et français sont parmi les plus ardents opposants au droit au chiffrement des communications.

Cette politique paranoïaque n'est pas seulement liberticide. Elle est également irresponsable. Car tandis que les gouvernements se focalisent sur la conservation généralisée des données de connexion et la cryptographie, le nécessaire débat sur les moyens de la lutte anti-terroriste est éludé. Après l'attaque de Londres, comme après chaque attentat, il a pourtant de nouveau été démontré que ce qu'il manque à l'antiterrorisme, ce sont notamment des moyens humains dédiés à l'analyse des données déjà recueillies dans le cadre de surveillances ciblées, et non pas des puits sans fond de données.

Aux autorités qui prétendent remédier à leurs échecs par toujours plus de mesures et de lois ineptes, tel le futur projet de loi antiterroriste, il faut opposer la construction d'un cadre juridique efficace et respectueux des libertés fondamentales, mais aussi des politiques publiques capables d'aborder le problème du terrorisme autrement que sous l'angle étroitement sécuritaire.

Faute de quoi, la fuite en avant délétère, décrite par M^{e} François Sureau lors d'une récente plaidoirie au Conseil constitutionnel, va se poursuivre : *« Après chaque attentat, les ministres bien intentionnés recommandent de continuer à se distraire, comme s'il s'agissait là d'un acte de résistance, alors que de l'autre main ils nous introduisent dans l'univers si commode pour eux, si dégradant pour nous, de la servitude administrative. Je ne sais rien de plus triste, ni de plus humiliant que cet abaissement et cette hypocrisie. »*

Les Exégètes amateurs sont un groupe d'action juridique bénévole commun à trois associations : La Quadrature du Net, French Data Network (FDN) et la Fédération des fournisseurs d'accès à Internet associatifs. Depuis janvier 2015, ils œuvrent devant les juridictions françaises et européennes, en faveur de la protection des libertés fondamentales telle que portée par ces associations. À l'initiative de ces dernières, une procédure est en cours devant le Conseil d'État depuis septembre 2015 pour faire appliquer la jurisprudence de la Cour de justice de l'Union européenne interdisant la conservation généralisée des données de connexion.

3. Tel fut le cas de la Roumanie en 2009, de l'Allemagne et de la Bulgarie en 2010, de Chypre et de la République Tchèque en 2011, de l'Autriche en 2014, de la Belgique, de la Finlande et des Pays-Bas en 2015 ainsi que de la Suède en 2017.