Données de connexion et usage d'algorithmes : les lois françaises en violation des droits fondamentaux

La justice européenne a déclaré illégales les dispositions françaises sur la conservation des données de trafic et de localisation par les opérateurs télécoms, ainsi que par les hébergeurs. Elle a aussi fourni une feuille de route sur l'utilisation de « boîtes noires » dans la lutte contre le terrorisme.

Par Winston Maxwell*, Telecom Paris, Institut polytechnique de Paris

La Cour de justice de l'Union européenne (CJUE) a, le 6 octobre 2020 (1), mis fin à un débat qui existe depuis le 8 avril 2014, date à laquelle elle avait annulé la directive de 2006 sur la conservation des données de trafic (2), estimant que celle-ci était contraire à la Charte des droits fondamentaux de l'UE (3). La CJUE a jugé que cette directive créait une atteinte disproportionnée au droit à la protection des données personnelles parce qu'elle exigeait la conservation généralisée et indifférenciée des données de trafic de l'ensemble de la population.

La France n'a pas (encore) bougé

La CJUE est intervenue une deuxième fois en 2016, annulant les dispositions britanniques et suédoises sur la conservation des données de trafic, précisant de nouveau qu'une obligation de conservation généralisée et indifférenciée était incompatible avec cette même Charte des droits fondamentaux (4). Malgré ces deux décisions de la justice européenne, la France n'a pas bougé, préservant sa législation qui impose, d'une part, la conservation par les opérateurs de communications électroniques des données de connexion et de localisation, et, d'autre part, la conservation par les hébergeurs des données relatives à l'identification des utilisateurs et à leurs activités sur les plateformes numériques.

En plus, après les attentats terroristes de 2015, la France a introduit de nouvelles mesures permettant aux autorités d'utiliser des « boîtes noires » pour analyser l'ensemble des données de trafic des réseaux. Et ce, afin de détecter des signaux faibles de projets terroristes.

La Quadrature du Net (5) a contesté l'ensemble de ces mesures devant le Conseil d'Etat, et celui-ci a envoyé plusieurs questions préjudicielles à la CJUE. Devant cette dernière, le gouvernement français a d'abord défendu sa législation sur le fondement de l'article 4 du Traité sur l'UE qui précise que la protection de la sécurité nationale relève de la compétence exclusive de la France. A titre subsidiaire, le gouvernement français a soutenu que la lutte contre le terrorisme justifiait des mesures de surveillance plus intrusives qu'en matière de criminalité simple, et que les dispositions françaises devaient dès lors être validées compte tenu du risque accru du terrorisme.

Sur le premier point, la CJUE a confirmé que le droit de l'UE ne s'appliquait pas aux activités de renseignement et de protection de la sécurité nationale entreprises par l'Etat lui-même. En revanche, lorsque l'Etat impose aux entreprises privées des obligations telles que la conservation de données, le droit de l'UE s'applique, même s'il s'agit de mesures destinées à lutter contre le terrorisme. Par conséquent, la jurisprudence de la CJUE dans les affaires précitées de 2014 « Digital Rights Ireland » et de 2016 « Tele2 Sverige et Watson » s'applique pleinement à la France.

La CJUE a été d'accord avec la France sur la nécessité d'accorder une marge de manœuvre plus grande aux Etats membres en matière de protection de la sécurité nationale, car la menace est d'une toute autre nature qu'en matière de criminalité.

Pour apprécier la proportionnalité de différentes mesures de surveillance, la CJUE établit trois niveaux de gravité :

• Le premier niveau est la protection de la sécurité nationale, y compris la lutte contre le terrorisme. Selon la CJUE, « *la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'Etat en tant que tel* », peut justifier une atteinte plus forte aux droits fondamentaux et, notamment, une obligation généralisée de conserver des données de trafic et de localisation. Mais cette obligation ne peut être justifiée que pendant une période limitée durant laquelle il existerait des « *circonstances suffisamment concrètes permettant de considérer que l'Etat (...) fait face à une menace grave* » pour sa sécurité nationale. Une commission indépendante ou un tribunal doit valider l'existence d'une telle menace.

Les trois niveaux de gravité

• Le deuxième niveau de gravité concerne la lutte contre la criminalité grave et les menaces graves contre la sécurité publique. Pour ce niveau, une obligation de conservation systématique et continue de données est exclue. Selon la CJUE, il faudrait qu'il existe un lien, même indirect, entre les données dont la conservation est demandée, et la détection ou la répression d'un crime grave. Ainsi, les demandes de conservation de données de trafic et de localisation doivent être ciblées, concernant un groupe particulier de personnes,

Notes

(1) - CJUE Affaires C-511/18, C-512/18 et C-520/18, La Quadrature du Net et autres, 6 octobre 2020.

(2) - Directive européenne 2006/24/CE : https://lc.cx/Directive Conservation2006

(3) - CJUE Affaire C-293/12 « Digital Rights Ireland », 8 avril 2014.

(4) - CJUE Affaire C-203/15 « Tele2 Sverige et Watson », 21 décembre 2016.

ou une zone géographie à risque, par exemple les données de trafic autour d'une gare. En revanche, s'il s'agit uniquement des adresses IP, ceux-ci peuvent être stockés de manière généralisée, selon la justice européenne.

• Le troisième niveau concerne toutes les formes de criminalité. Seul le stockage des données relatives à l'identité civile des utilisateurs peut être envisagé. La conservation d'autres données est exclue.

Cette approche graduée découle naturellement de la jurisprudence de la CJUE en matière de proportionnalité – plus la menace pour l'Etat et les citoyens est élevée, plus le niveau d'ingérence avec la vie privée peut être élevé.

Algorithmes de détection en temps réel

La France devra donc réécrire ses lois pour introduire une différenciation entre les menaces graves pour la sécurité nationale (menaces de niveau 1), menaces graves pour la sécurité publique et lutte contre la criminalité grave (menaces de niveau 2), et lutte contre la criminalité ordinaire (menaces de niveau 3). A chaque niveau correspondra des règles adaptées en matière de conservation des données.

L'autre leçon de la décision de la CJUE concerne la régulation des algorithmes utilisés par l'administration française pour détecter des projets terroristes. Depuis la loi de 2015 sur les techniques de renseignement (6), les services spécialisés – désignés par décret en Conseil d'Etat – ont la possibilité de procéder à l'analyse automatique des données de trafic et de localisation en temps réel afin de détecter des signaux faibles d'activités terroristes. Cette possibilité est strictement encadrée par la Commission nationale de contrôle des techniques de renseignement (CNCTR (7)), et la période d'expérimentation doit prendre fin le 31 juillet 2021. Le gouvernement a récemment proposé d'étendre la période d'expérimentation des algorithmes jusqu'à fin décembre 2021.

L'utilisation de l'intelligence artificielle pour lutter contre le terrorisme est controversée, car les algorithmes sont faillibles et peuvent tirer des conclusions erronées et discriminatoires. Dans sa décision du 6 octobre, la CJUE fournit une feuille de route sur la possibilité de déployer ces outils.

D'abord, la justice européenne confirme que l'analyse des données de trafic et de localisation en temps réel constitue une ingérence *« particulièrement grave »* avec la protection de la vie privée. Le déploiement d'un tel dispositif doit être prévu par une loi claire et précise qui définit les limites et les mesures de protection accompagnant le dispositif. La CJUE indique que le dispositif ne peut se justifier qu'en présence d'une menace grave pour la sécurité nationale qui s'avère *« réelle et actuelle ou prévisible »*. Un tribunal ou autorité administrative indépendante doit contrôler l'existence d'une telle menace, et ses décisions doivent avoir un effet contraignant. En ce qui concerne l'algorithme lui-même, les modèles et critères préétablis doivent être *« spécifiques et fiables, permettant d'aboutir à des résultats identifiant des individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes et, d'autre part, non discriminatoires »*. Les modèles et critères préétablis ne peuvent se fonder seulement sur des données sensibles.

Les termes utilisés par la CJUE suggèrent que l'algorithme pourrait éventuellement s'appuyer – en partie – sur des données sensibles, ce qui semble en contradiction avec le règlement général sur la protection des données (RGPD) en vigueur au niveau européen. La CJUE indique ensuite que tout algorithme comporte un taux d'erreur, et que tout résultat positif doit être soumis à un réexamen individuel par un analyste humain avant la mise en œuvre d'autres mesures de surveillance. Cette exigence de la CJUE pose la question de la compréhension de la recommandation algorithmique par l'analyste humain et sa capacité de contredire l'algorithme. Pour qu'il y ait une vraie intervention humaine, l'algorithme doit être en mesure d'expliquer pourquoi il a détecté des signaux faibles d'activités terroristes, et l'analyste humain doit être en mesure d'apporter une analyse critique par rapport à l'explication donnée par l'algorithme. Lorsque l'algorithme s'appuie sur des techniques d'apprentissage-machine *(machine learning)*, de telles explications peuvent s'avérer difficiles.

La CJUE impose un réexamen régulier de l'algorithme et les données utilisées pour garantir l'absence de discrimination et le caractère strictement nécessaire du dispositif à la lumière de la menace terroriste. La fiabilité et l'actualité des modèles et critères préétablis, et les bases de données utilisées, doivent également être revues régulièrement par une autorité de contrôle, soit une forme de suivi dynamique. Enfin, si l'algorithme débouche sur la surveillance plus poussée d'un individu, celui-ci doit être informé dès le moment où cette communication n'est pas susceptible de compromettre les missions incombant aux autorités.

Renseignement : la loi française à réécrire

Réunie le 7 juillet 2020, la commission de la Défense nationale et des Forces armées de l'Assemblée nationale a estimé que le recours aux algorithmes était utile et nécessaire dans lutte contre le terrorisme et devrait être pérennisé, voire étendu pour permettre l'analyse d'autres données, telles que des URL (8) de sites web consultés (9). Au moment de sa séance, la commission parlementaire avait connaissance de l'affaire pendante devant la CJUE et a reconnu que celle-ci pourrait avoir un profond impact sur les méthodes utilisées en France. Elle ne s'y est pas trompée : la décision du 6 octobre impose une réécriture de la loi française sur les techniques de renseignement. @

* Winston Maxwell, ancien avocat, est depuis juin 2019 directeur d'études Droit et Numérique à Telecom Paris.

Notes

(5) - La Quadrature du Net (LQDN) est une association française de défense des droits et libertés numériques.

(6) - Loi n°2015-912 du 24 juillet 2015 relative au renseignement.

(7) - https://www.cnctr.fr/

(8) - Uniform Resource Locator (URL), à savoir l'adresse web.

(9) - Compte rendu : https://lc.cx/CDNFA-0707620