La lutte contre le terrorisme contrariée par un arrêt européen

L'application d'une décision de la Cour de justice sur le stockage des données personnelles pourrait mettre à mal une partie des enquêtes

Une décision très ennuyeuse pour les services de police, de renseignement et la justice, particulièrement dans le cadre de la lutte antiterroriste, agite depuis plusieurs mois les cabinets ministériels. Passée inaperçue du grand public, elle émane de la Cour de justice de l'Union européenne (CJUE) et est tombée quatre jours avant Noël. Son objet : restreindre les conditions d'accès aux données conservées par les opérateurs de téléphonie ou les fournisseurs d'accès à Internet. Un enjeu technique mais crucial, à l'heure où les enquêtes sont de plus en plus dépendantes de l'analyse des communications et du réseau des victimes ou des suspects.

Le dossier, sensible, est, selon nos informations, d'ores et déjà en bonne place sur le bureau du nouveau ministre de l'intérieur, Gérard Collomb. Alors qu'Emmanuel Macron a annoncé vouloir présidentialiser un peu plus la lutte contre le terrorisme en créant une *« task force anti-Daech »* lui étant directement rattachée à l'Elysée, il devrait aussi rapidement lui remonter.

« Ingérence » dans « la vie privée »

Cette décision de la CJUE en date du 21 décembre 2016 prévoit que seule une *« menace grave »* peut désormais justifier la conservation des données par les opérateurs et les fournisseurs d'accès à Internet (FAI). Autrement dit, finie la conservation *« indifférenciée »* à titre préventif, comme c'est le cas actuellement partout en Europe. A écouter la CJUE, impossible à l'avenir de continuer d'y piocher au gré des investigations.

En France, cette conservation « indifférenciée » des données de trafic ou de localisation est encadrée et autorisée juste pour une durée d'un an. Mais si la décision de la CJUE est appliquée *stricto sensu*, même ce stockage ne sera plus possible. Pour la CJUE, depuis décembre, tout doit être en principe limité *« au strict nécessaire »* et de surcroît *« conservé sur le territoire national »*. Au risque sinon, selon elle, de constituer une *« ingérence »* disproportionnée dans *« la vie privée »* des citoyens.

Une gageure toutefois, aux yeux des milieux concernés. Chez les policiers et magistrats – y compris chez les plus ouverts à la protection des données personnelles –, nul ne sait comment mettre en œuvre cette décision. L'interprétation des arrêts de la CJUE est toujours un exercice en soi. En pratique, il appartient aux juridictions nationales de trancher la manière dont ils vont être transposés. Sauf que, jusqu'à présent, personne n'a vu comment s'y plier sans faire tomber toutes les enquêtes en cours et empêcher toutes celles à venir... Cornélien à l'heure où la menace terroriste demeure au plus haut.

Au cœur des difficultés : le fait de réussir à définir, au préalable, quels individus relèveraient d'une « menace grave » ou pas. *« Il n'y a que dans* Minority Report [film de science-fiction de Steven Spielberg] *que l'on peut savoir a priori sur qui l'on va enquêter »*, tempête un policier de haut rang. *« Si la jurisprudence de la CJUE se confirme sur ce point, cela va vraiment poser problème »*, confirme François-Xavier Masson, le patron de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Le malaise est aussi palpable dans le monde du renseignement. Dans son dernier rapport annuel, publié en avril, la délégation parlementaire au renseignement pointait les *« incertitudes »* et le *« problème »* de l'arrêt de la CJUE. *« Il empiète sur la compétence des Etats et ne tient manifestement aucun compte des impératifs et des finalités qui s'attachent à l'action des services de renseignement »*, écrivaient les parlementaires chargés du contrôle des services.

En 2014, la CJUE avait déjà rendu un arrêt similaire (dit « Digital Rights »). Arrêt qu'une entreprise suédoise avait décidé d'appliquer elle-même dès le lendemain, pour éviter d'avoir à stocker des données. Le gouvernement suédois s'y était alors opposé, déclenchant une procédure qui aboutit à la décision actuelle, dite « Tele2 ».

Jusqu'à présent, personne n'a vu comment se plier à cette décision sans faire tomber les enquêtes en cours et empêcher celles à venir...

Interrogé par *Le Monde*, le ministère de l'intérieur se veut rassurant. *« Il n'y a pas de conséquences immédiates pour les services de renseignements car cette décision n'est pas directement applicable au regard des nombreuses garanties qui encadrent l'accès aux données dans notre pays »*, explique-t-on. Comme tous les Etats membres devront s'y plier, l'arrêt de la CJUE *« fait actuellement l'objet d'une réflexion avec nos partenaires européens dans un souci de clarification »*, précise-t-on aussi, prudent, sachant que des recours de militants des libertés individuelles pourraient rapidement s'engouffrer dans la brèche.

Concrètement, les données conservées actuellement par les opérateurs et les FAI – pour une durée de six mois à deux ans selon les pays – concernent seulement les éléments de connexions (identifiants, nom, adresse mail, etc.), pas le contenu des conversations. Des données toutefois jugées indispensables dans les cercles opérationnels. *« C'est la matière première,* plaide un enquêteur, *dans toutes les enquêtes nous avons besoin, à un moment ou à un autre, de recourir aux données conservées par les opérateurs pour identifier ou localiser un mis en cause, un complice, voire une victime. »*

« Collecte massive »

« Avant les moyens modernes de communication, les personnes ayant des projets criminels pouvaient difficilement élaborer leurs plans à distance, donc elles se rencontraient. Maintenant il y a de moins en moins de contacts physiques. Les moyens (Internet, smartphone) ont évolué, en contrepartie, il faut que l'on puisse les suivre », estime un autre policier spécialisé, rappelant que toutes les investigations sont faites sous le contrôle d'un magistrat pour les investigations judiciaires ou d'une autorité administrative indépendante pour les services de renseignement.

Même la Commission nationale de l'informatique et des libertés (CNIL), l'autorité chargée de la protection des données personnelles, ne sait aujourd'hui pas par quel bout prendre la décision européenne. *« Nous sommes en train d'expertiser cet arrêt »*, a expliqué au *Monde*, le 27 mars, sa présidente, Isabelle Falque-Pierrotin, lors de la présentation du rapport annuel : *« L'analyse de la cour est, sur le plan opérationnel, difficile à mettre en œuvre, car lorsqu'on collecte des données auxquelles il est possible, le cas échéant, d'accéder, vous ne connaissez pas toujours la finalité en amont. » « Nous pensons que c'est un arrêt sur lequel il faut réfléchir. Il illustre la volonté politique de la Cour européenne de dire que la collecte massive et indifférenciée de données n'est pas possible »*, a-t-elle cependant estimé.

Outre l'administration, la justice devra aussi tirer les conséquences de l'arrêt Telez. Plusieurs contentieux lancés dans l'Hexagone, en cours d'instruction, vont pouvoir s'appuyer sur le raisonnement des juges européens. Le premier, lancé en mai 2015, vise le code des postes et des communications électroniques, notamment sa partie encadrant la rétention des données. L'autre concerne la loi renseignement de 2015. Dans les deux cas, la balle est dans le camp du Conseil d'Etat. ■

MARTIN UNTERSINGER ET ÉLISE VINCENT

Un précédent sur l'immigration

Ce n'est pas la première fois qu'un arrêt de la Cour de justice de l'Union européenne (CJUE) pose des problèmes d'application cornéliens aux Etats membres. Des écarts d'appréciation du réel qui conduisent régulièrement au contournement des décisions de la Cour par des subtilités juridiques. En matière d'immigration, par exemple, en 2011 et 2012, la CJUE avait rendu deux arrêts considérant que le séjour irrégulier d'un étranger n'était plus un « délit ». Ce qui mettait de facto par terre tout le système d'éloignement des étrangers. La France s'était bien pliée à l'arrêt en supprimant la possibilité de placer en garde à vue durant quarante-huit heures un étranger au seul motif qu'il était en séjour irrégulier. Mais, par une loi de décembre 2012, elle avait créé un régime à mi-chemin, permettant malgré tout de faire des vérifications d'identité : « la retenue administrative », d'une durée de seize heures maximum.