Nomos
société d'avocats

nomosnetcom.fr **Janvier 2017**

La CJUE se prononce contre les obligations de conservation généralisée des données de connexion

[DONNÉES PERSONNELLES]
CJUE, 21 décembre 2016, Tele2 Sverige AB c/ Post-och telestyrelsen & Secretary of State for the Home Department c/ Tom Watson

L'accès aux métadonnées se rapportant aux diverses formes de communications électroniques suscite un intérêt particulier pour les Etats, notamment aux fins de lutte contre la criminalité, le terrorisme, mais également dans le cadre du renseignement « normal ». Ce n'est que récemment, avec les révélations d'Edward Snowden, que ces questions ont été appréhendées par le grand public et les médias. Mécaniquement, le cadre juridique existant et les pratiques étatiques sont désormais attentivement scrutés, menant à de nombreuses actions en justice.

C'est dans ce contexte que, le 8 avril 2014, la CJUE a rendu l'arrêt très remarqué « *Digital Rights* », par lequel elle a invalidé la directive 2006/24 portant sur : « *la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications* ». Cette directive imposait aux Etats membres de prévoir l'obligation, pour les fournisseurs de services de communication électronique, de conserver et rendre accessible un certain nombre de métadonnées se rapportant aux communications électroniques (source, destinataire, date, heure, durée, type, matériel utilisé et localisation). Or, la Cour relevait que la directive ne comprenait aucune limite aussi bien concernant les personnes, les moyens de communication et les données concernées. D'autre part, l'accès aux données était trop large et rien ne garantissait que la durée de leur conservation soit limitée au strict nécessaire. A cela s'ajoutait l'absence de garantie suffisante en matière de sécurité et l'absence d'obligation de conserver les données au sein de l'U.E. En conséquence, la CJUE considérait que la directive contrevenait notamment aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union Européenne, protégeant respectivement la vie privée et les données personnelles.

Bien que l'arrêt « *Digital Rights* » ait comporté quelques considérations de portée générale, l'invalidation de la directive n'a pas eu de conséquence directe sur les législations des Etats membres. Cependant, cet arrêt a logiquement inspiré de nouvelles actions portant cette fois-ci sur les règlementations nationales, inspirées de la directive invalidée. C'est dans ce contexte que s'inscrit l'arrêt *« Tele2* » rendu par la CJUE le 21 décembre 2016.

Cet arrêt regroupe deux affaires distinctes. Dans la première, un fournisseur d'accès suédois avait cessé de conserver les données de trafic de ses abonnés sur le fondement de l'arrêt « *Digital Rights* », et ce en violation de la loi suédoise. Dans la seconde, trois personnes avaient introduit un recours contre la loi anglaise dont les dispositions étaient identiques à la directive invalidée. La question préjudicielle principale à laquelle a dû répondre la CJUE était la suivante : une règlementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation, ainsi que l'accès à ces données par les autorités nationales, est-elle compatible avec le droit de l'U.E. ?

Plusieurs dispositions du droit de l'U.E. ont été analysées par la Cour. En effet, la directive 2002/58 « *Vie privée et communications électroniques* » pose l'obligation générale d'effacer ou de rendre anonymes les données relatives au trafic lorsque celles-ci ne sont plus nécessaires à la transmission de la communication (articles 5 et 6). Cependant, la directive prévoit également la possibilité pour les Etats membres de déroger à ces principes, notamment en adoptant des « *mesures législatives prévoyant la conservation des données pendant une durée limitée* » (article 15§1). La CJUE a donc dû confronter les législations nationales en cause à ces textes, eux-mêmes lus à la lumière des articles 7 (protection de la vie privée), 8 (protection des données personnelles) et 52§1 (principe de proportionnalité et de nécessité des exceptions) de la Charte des droits fondamentaux de l'U.E.

Tout d'abord, la Cour confirme que les législations en cause, qui ont pour finalité déclarée la lutte contre la criminalité, relèvent bien du champ d'application de la directive 2002/58. En effet, certains pays (au rang desquels la France) étaient intervenus en relevant que l'article 1§3 de la directive excluait les « activités des Etats » se rapportant à la sécurité publique, la défense ou la sûreté de l'Etat, ainsi que celles concernant le droit pénal. Cependant, il ressort de l'article 15§1 de cette même directive que les Etat membres pouvaient déroger au texte pour des finalités recoupant les domaines visés à l'article 1§3. C'est donc que de telles mesures prises « par exception » relèvent bien en principe du champ de la directive, au risque de priver l'article 15§1 de tout effet utile.

Sur le fond, la Cour rappelle que l'article 15§1 de la directive 2002/58 ne permet de déroger à l'interdiction de conserver les données de trafic que lorsque ladite dérogation est « *nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques* ». La Cour estime ensuite que bien qu'il s'agisse de métadonnées et non du contenu même des communications, ces données sont susceptibles de permettre de tirer des « *conclusions très précises concernant la vie privée des personnes dont les données ont été conservées* ». En conséquence, la conservation de telles données constitue pour la Cour une ingérence grave dans les droits fondamentaux des personnes concernées, qui ne pourrait en tout état de cause être justifiée que par la lutte contre la criminalité grave.

Or, la Cour observe que la règlementation nationale en cause, bien que justifiée par la lutte contre la criminalité « *prévoit une conservation généralisée et indifférenciée de l'ensemble des données de trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communications électroniques, et qu'elle oblige les fournisseurs de services de communication électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception* ». En conséquence, la Cour considère qu'une telle règlementation excède les limites du strict nécessaire et ne saurait être considérée comme conforme aux conditions posées par l'article 15§1 de la directive 2002/58, lu à la lumière de la Charte des droits fondamentaux de l'U.E.

Pour respecter le droit de l'U.E., de telles règlementations doivent donc être ciblées, limitées, et fondées sur des éléments objectifs, tant en ce qui concerne les catégories de données, les moyens de communication visés, que les personnes concernées et la durée de conservation. D'autre part, les données devraient être conservées sur le territoire de l'U.E. et leur accès devrait en principe être subordonné à un contrôle préalable du juge ou d'une entité indépendante.

Cette décision ne devrait pas être sans répercussion en France, qui dispose de plusieurs articles ayant trait à la conservation des données de connexion, et notamment :

- L'article L34-1 du Code des postes et des communications électroniques : pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ;
- L'article 6 II de la loi « *LCEN* » : sur la conservation des données de nature à permettre l'identification de quiconque a contribué à la création de contenu en ligne ;
- La loi renseignement et ses fameuses « boites noires » devant permettre la détection et la conservation des données de connexion et de localisation en cas de menace terroriste.

Il convient en particulier de mentionner l'action en cours devant le Conseil d'Etat, formée par le groupe des « Exégètes » (regroupant la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à Internet associatifs), contre les décrets d'application des deux premiers textes cités ci-dessus. Le nouvel arrêt de la CJUE devrait logiquement alimenter l'argumentation des requérants, dont l'action est d'ores et déjà directement inspirée de l'arrêt *« Digital Rights »*.

Sylvain NAILLAT