COUR DE JUSTICE DE L'UNION EUROPEENNE – RENVOI PREJUDICIEL, 21 DECEMBRE 2016, AFFAIRES JOINTES TELE2 SVERIGE AB C/ POST- OCH TELESTYRELSEN (C-203/15), ET SECRETARY OF STATE FOR THE HOME DEPARTMENT C/ TOM WATSON (C-698/15)

MOTS CLEFS : internet – vie privée – confidentialité des communications électroniques – traitement des données à caractère personnel – données relatives au trafic – données de localisation – interdiction d'une conservation généralisée et indifférenciée – sécurité

La Cour de Justice de l'Union Européenne a déjà eu à traiter de la validité de l'obligation générale de conservation des données relatives au trafic et des données de localisation imposée par la directive de 2006 sur la conservation des données. Par un arrêt Digital Rights Ireland de 2014, la Cour a invalidé ladite directive au motif que l'ingérence que génère l'obligation précitée n'était pas limitée au strict nécessaire. Par la suite, la Cour de Justice a été saisie de deux affaires portant sur l'obligation générale imposée, en Grande-Bretagne comme en Suède, aux fournisseurs de services de communications électroniques de conserver les données relatives à ces communications. La réponse apportée par la Cour est claire, les États membres ne peuvent pas imposer une obligation générale de conservation généralisée et indifférenciée de données aux fournisseurs de services de communications électroniques, sauf si cette obligation est ciblée et limitée au strict minimum.

FAITS : Sur la base de la directive de 2006 invalidée par la Cour de Justice de l'Union Européenne, la Suède et la Grande-Bretagne prévoyaient une règlementation similaire qui obligeait les opérateurs de télécommunications à conserver systématiquement les données relatives au trafic et des données de localisation de leurs abonnés, respectivement pour une durée maximale de six et douze mois. Mais d'un côté, l'entreprise Tele2Sverige, fournisseur de services de communications électroniques établie en Suède, indique aux autorités suédoises qu'elle cessera de conserver lesdites données. Et d'un autre côté, des citoyens britanniques, MM. Watson, Brice et Lewis, forment un recours juridictionnel contre le régime britannique de conservation des données.

PROCEDURE : Une injonction de conservation des données a été adressée à Tele2Sverige qui a alors introduit un recours devant la juridiction administrative nationale, sans succès, avant d'interjeter appel. Parallèlement en Grande Bretagne, suite au recours des citoyens précités le Ministre de l'Intérieur a saisi la juridiction d'appel. La Cour de Justice de l'Union Européenne a alors été saisie par voie préjudicielle simultanément par les juridictions d'appel suédoise et britannique. Dans la mesure où les questions qui lui ont été soumises sont similaires, la Cour a décidé de les traiter conjointement.

PROBLEME DE DROIT : La question soumise aux juges européens était de savoir si les règlementations nationales qui imposent aux fournisseurs de services de communications électroniques une obligation générale de conservation des données, dans le but de les transmettre aux autorités nationales, sont compatibles avec le droit de l'Union européenne.

SOLUTION : La Cour de Justice de l'Union Européenne rappelle que le droit de l'Union s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, ainsi elle juge que les États membres ne peuvent pas imposer une obligation générale de conservation de ces données aux fournisseurs de services de communications électroniques. Concernant de telles données la Cour admet seulement une conservation ciblée, visant à lutter contre la criminalité grave, et limitée au strict nécessaire.

Cette création par LID2MS-IREDIC est mise à disposition selon les termes de la licence Creative Commons Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.0 France.

NOTE :

La demande des requérants suédois et britanniques portait sur la compatibilité de leur règlementation nationale avec le droit de l'Union européenne. Ces règlementations nationales sont similaires et imposent aux fournisseurs de services de communications électroniques une obligation générale de conservation des données relatives aux données de connexion.

La Cour de Justice de l'Union Européenne rappelle justement que le droit de l'Union s'oppose à une telle pratique, notamment la directive « vie privée et communications électroniques » de 2002 ainsi que la Charte des droits fondamentaux. Mais ladite Cour admet une conservation ciblée uniquement dans le but de lutter contre la criminalité grave et le terrorisme, et à condition qu'elle soit limitée au strict nécessaire concernant à la fois les catégories de données à conserver, les moyens de communication visés, les personnes concernées et la durée de conservation choisie.

Une solution en adéquation avec la jurisprudence établie

Ainsi, la Cour de Justice vient logiquement censurer des règlementations nationales prises sur la base de la directive de 2006 sur la conservation des données, invalidée en 2014 par son arrêt Digital Rights Ireland.

En effet, comme dans sa jurisprudence précédente, la Cour de Justice de l'Union Européenne explique que l'ingérence que comporte cette obligation de conservation de données généralisée et indifférenciée porte atteinte aux droits fondamentaux des citoyens européens, notamment au respect de leur vie privée et à la protection de leurs données à caractère personnel. Un argument incontestable tant les règlementations nationales en cause contreviennent à ces droits fondamentaux.

Les juges européens confirment donc leur raisonnement employé en 2014, une conservation généralisée et indifférenciée des données de connexion, même assortie de garanties légales, est trop dangereuse pour la vie privée des individus.

Une solution favorable à la liberté des individus plutôt qu'à la sécurité

Dès lors, il apparait que la Cour de Justice de l'Union Européenne fait primer le principe du respect de la vie privée des particuliers sur le principe d'intérêt général des Etats relatif à la lutte contre le terrorisme et la criminalité grave. Toutefois, la Cour de Justice a fait preuve de mesure en acceptant une conservation des données de connexion d'une catégorie identifiée d'individus. Les juges ont pris en compte le climat actuel qui sévit en Europe, et par cette exception ils autorisent les Etats membres à agir en amont face à la menace terroriste et la criminalité grave. Il convient de saluer cette solution visant à protéger la liberté même si l'on peut douter de l'efficacité des moyens mis à la disposition des Etats membres pour lutter contre ces menaces.

S'agissant de l'accès des autorités nationales aux données conservées par les fournisseurs de services, les juges européens précisent justement que cet accès sera soumis à certaines conditions. Ainsi, l'accès sera soumis à un contrôle préalable par une autorité indépendante afin de vérifier si les données sont transmissibles, et la Cour exige également que la conservation des données se fasse sur le territoire de l'Union européenne. Des garanties visant à s'assurer que la communication de telles données se fasse uniquement dans un but de sécuriser les territoires européens et leurs citoyens.

Dès lors il apparait clairement que même si la Cour de Justice tient compte du fait que les Etats ont besoin d'être dotés d'outils leur permettant de lutter contre le terrorisme et la criminalité, elle ne le fait pas au détriment de la vie privée de l'ensemble des individus européens.

Thomas Rouillé
Master 2 Droit des médias et des télécommunications
AIX-MARSEILLE UNIVERSITE, LID2MS-IREDIC 2017

Cette création par LID2MS-IREDIC est mise à disposition selon les termes de la licence Creative Commons Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.0 France.

ARRET :

CJUE, 21 décembre 2016, C-203/15 et C-698/15

1. Les demandes de décision préjudicielle portent sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive 2002/58 »), lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») […]

97. S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause dans l'affaire C-203/15, satisfait à ces conditions, il convient de relever que celle-ci prévoit une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception. Ainsi qu'il ressort de la décision de renvoi, les catégories de données visées par cette réglementation correspondent, en substance, à celles dont la conservation était prévue par la directive 2006/24 […]

99. Prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 27). En particulier, ces données fournissent les moyens d'établir […] le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications […]

100. L'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante [...]

108. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition 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 […]

119. […] À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction […].

Cette création par LID2MS-IREDIC est mise à disposition selon les termes de la licence Creative Commons Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.0 France.