Presse et Information

Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 145/16
Luxembourg, le 21 décembre

Arrêt dans les affaires jointes C-203/15 Tele2 Sverige AB/ Post-och telestyrelsen et C-698/15 Secretary of State for the Home Department/Tom Watson e.a.

Les États membres ne peuvent pas imposer une obligation générale de conservation de données aux fournisseurs de services de communications électroniques

Le droit de l'Union s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, mais il est loisible aux États membres de prévoir, à titre préventif, une conservation ciblée de ces données dans le seul but de lutter contre la criminalité grave, à condition qu'une telle conservation 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. L'accès des autorités nationales aux données conservées doit être soumis à des conditions, dont notamment un contrôle préalable par une autorité indépendante et la conservation des données sur le territoire de l'Union

Dans son arrêt Digital Rights Ireland de 2014[1], la Cour de justice a invalidé la directive sur la conservation des données[2] au motif que l'ingérence que comporte l'obligation générale de conservation des données relatives au trafic et des données de localisation imposée par celle-ci dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel n'était pas limitée au strict nécessaire.

À la suite de cet arrêt, la Cour a été saisie de deux affaires portant sur l'obligation générale imposée, en Suède et au Royaume-Uni, aux fournisseurs de services de communications électroniques de conserver les données relatives à ces communications, dont la conservation était prévue par la directive invalidée.

Le lendemain du prononcé de l'arrêt Digital Rights Ireland, l'entreprise de télécommunication Tele2 Sverige a notifié à l'autorité suédoise de surveillance des postes et télécommunications sa décision de cesser de procéder à la conservation des données ainsi que son intention d'effacer les données déjà enregistrées (affaire C-203/15). Le droit suédois oblige en effet les fournisseurs de services de communications électroniques à conserver de manière systématique et continue, et ce sans aucune exception, l'ensemble des données relatives au trafic et des données de localisation de tous leurs abonnés et utilisateurs inscrits, concernant tous les moyens de communication électronique.

Dans l'affaire C-698/15, MM. Tom Watson, Peter Brice et Geoffrey Lewis ont introduit des recours contre le régime britannique de conservation des données qui permet au ministre de l'Intérieur d'obliger les opérateurs de télécommunications publiques à conserver toutes les données relatives à des communications pour une durée maximale de douze mois, étant entendu que la conservation du contenu de ces communications est exclue.

Saisie par le Kammarrätten i Stockholm (cour administrative d'appel de Stockholm, Suède) et la Court of Appeal (England and Wales) (Civil Division) (chambre civile de la cour d'appel d'Angleterre et du pays de Galles, Royaume-Uni), la Cour est invitée à indiquer si des régimes

[1] Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.* (affaires jointes C-293/12 et C-594/12, voir CP n° 54/14).
[2] Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, 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, et modifiant la directive 2002/58/CE (JO L 105, p. 54).

nationaux qui imposent aux fournisseurs une obligation générale de conservation des données et qui prévoient l'accès des autorités nationales compétentes aux données conservées, sans notamment limiter cet accès aux seules fins de lutte contre la criminalité grave et soumettre l'accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, sont compatibles avec le droit de l'Union (en l'occurrence la directive « vie privée et communications électroniques »[3] lue à la lumière de la Charte des droit fondamentaux de l'UE[4]).

Dans son arrêt de ce jour, **la Cour répond que le droit de l'Union s'oppose à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données.**

La Cour confirme tout d'abord que **les mesures nationales** en cause **relèvent du champ d'application de la directive.** En effet, la protection de la confidentialité des communications électroniques et des données relatives au trafic, garantie par la directive, s'applique aux mesures prises par toute personne autre que les utilisateurs, qu'il s'agisse de personnes ou d'entités privées ou d'entités étatiques.

La Cour constate ensuite que, si cette directive permet aux États membres de limiter la portée de l'obligation de principe d'assurer la confidentialité des communications et des données relatives au trafic y afférentes, elle ne saurait justifier que la dérogation à cette obligation de principe et, en particulier, à l'interdiction de stocker ces données, prévue par celle-ci, devienne la règle.

En outre, la Cour rappelle sa jurisprudence constante selon laquelle la protection du droit fondamental au respect de la vie privée exige que **les dérogations** à la protection des données à caractère personnel **s'opèrent dans les limites du strict nécessaire**. La Cour applique cette jurisprudence aux règles régissant la conservation des données et à celles régissant l'accès aux données conservées.

La Cour constate, **s'agissant de la conservation**, que les données conservées prises dans leur ensemble **sont susceptibles de permettre de tirer des conclusions très précises sur la vie privée des personnes** dont les données ont été conservées.

L'ingérence résultant d'une réglementation nationale prévoyant la conservation des données relatives au trafic et des données de localisation doit donc être considérée comme particulièrement grave. Le fait que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques n'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. Par conséquent, **seule la lutte contre la criminalité grave est susceptible de justifier une telle ingérence**.

La Cour relève qu'une **réglementation prévoyant une conservation généralisée et indifférenciée des données ne requiert pas de relation entre les données dont la conservation est prévue et une menace pour la sécurité publique** et ne se limite notamment pas à prévoir une conservation des données afférentes à une période temporelle et/ou une zone géographique et/ou un cercle de personnes susceptibles d'être mêlées à une infraction grave. **Une telle réglementation nationale excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique, ainsi que l'exige la directive lue à la lumière de la Charte.**

La Cour explique en revanche que **la directive ne s'oppose pas à une réglementation nationale imposant une conservation ciblée des données** à des fins de lutte contre la criminalité grave**, à condition qu'une telle conservation soit**, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que

[3] 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 L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO L 337, p. 11).

[4] Articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne.

la durée de conservation retenue, **limitée au strict nécessaire**. Selon la Cour, **toute réglementation nationale allant dans ce sens doit être claire et précise** et **prévoir des garanties suffisantes** afin de protéger les données contre les risques d'abus. Elle doit indiquer les circonstances et conditions dans lesquelles une mesure de conservation des données peut, à titre préventif, être prise, de manière à garantir que l'ampleur de cette mesure soit, en pratique, effectivement limitée au strict nécessaire. Notamment, une telle réglementation doit être **fondée sur des éléments objectifs** permettant de viser les personnes dont les données sont susceptibles de présenter un lien avec des actes de criminalité grave, de contribuer à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique.

S'agissant de **l'accès des autorités nationales compétentes aux données conservées**, la Cour confirme que la réglementation nationale concernée ne saurait se limiter à exiger que l'accès réponde à l'un des objectifs visés à la directive, fût-ce la lutte contre la criminalité grave, mais doit également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées. Cette réglementation doit se fonder sur des **critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé aux autorités nationales compétentes**. Un accès ne saurait en principe être accordé, s'agissant de 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. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités.

De plus, la Cour considère **qu'il est essentiel que l'accès aux données conservées soit, sauf en cas d'urgence, subordonné à un contrôle préalable** effectué par une juridiction ou une entité indépendante. En outre, les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé doivent en informer les personnes concernées.

Compte tenu de la quantité de données conservées, du caractère sensible de ces données ainsi que du risque d'accès illicite à celles-ci, **la réglementation nationale doit prévoir que les données soient conservées sur le territoire de l'Union** et qu'elles soient irrémédiablement détruites au terme de la durée de leur conservation.

RAPPEL: Le renvoi préjudiciel permet aux juridictions des États membres, dans le cadre d'un litige dont elles sont saisies, d'interroger la Cour sur l'interprétation du droit de l'Union ou sur la validité d'un acte de l'Union. La Cour ne tranche pas le litige national. Il appartient à la juridiction nationale de résoudre l'affaire conformément à la décision de la Cour. Cette décision lie, de la même manière, les autres juridictions nationales qui seraient saisies d'un problème similaire.

Contact presse: Gilles Despeux ☎ (+352) 4303 3205