COUR DE JUSTICE DE L'UNION EUROPEENNE (GRANDE CHAMBRE) – PREMIERES QUESTIONS PREJUDICIELLES DANS LES AFFAIRES C-511/18 ET C-512/18, PREMIERE ET DEUXIEME QUESTIONS PREJUDICIELLES DANS L'AFFAIRE C-520/18, 6 OCTOBRE 2020

MOTS CLEFS : CJUE – données personnelles – conservation – fournisseurs d'accès à Internet – directive vie privée et communications électroniques – sécurité nationale

Si la confidentialité des communications électroniques et des données relatives au trafic demeure le principe défendu par la directive 2002/58, celles-ci sont devenues des enjeux majeurs du renseignement, notamment en matière de terrorisme. Certains législateurs nationaux, à l'image du législateur français, ont alors enjoint aux fournisseurs d'accès de conserver sans limite les données afférentes aux communications en ligne. Toutefois, comme le rappelle la Cour de Justice de l'Union Européenne (CJUE) par la présente décision, une telle obligation est contraire au droit de l'Union. La Cour tempère toutefois le propos, apportant des nuances en fonction des données en cause, de leurs modalités de recueil, et des motifs invoqués.

FAITS : La législation française, par des dispositions inscrites au sein du Code des postes et des communications électroniques et du Code de la sécurité intérieure, prévoit l'obligation pour les fournisseurs d'accès d'une conversation généralisée des données de connexion. Le droit belge prévoit des mesures similaires.

PROCEDURE : Différentes associations françaises ont porté un recours devant le Conseil d'État contre ces mesures, estimant qu'il s'agissait d'ingérences injustifiées dans les droits fondamentaux des personnes. Des associations ont mené une procédure similaire devant la Cour constitutionnelle belge. Les deux juridictions ont alors effectué un renvoi préjudiciel devant la CJUE, interrogeant notamment le juge européen sur le caractère justifiable de ces mesures au regard du contexte et des objectifs poursuivis, à savoir la sécurité nationale et la lutte contre le terrorisme. La CJUE a rendu, le 6 octobre 2020, une décision regroupant ces affaires.

PROBLEME DE DROIT : L'ingérence dans le droit au respect de la vie privée et le droit à la protection des données personnelles, constituée par l'obligation de conservation généralisée et indifférenciée des données faite aux fournisseurs d'accès, se justifie-t-elle au regard du droit à la sûreté et des exigences de la sécurité nationale ?

SOLUTION : Par la présente décision, la CJUE réaffirme l'interdiction d'une transmission ou d'une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation. Toutefois, la mise en balance des intérêts en cause implique que dans un contexte de menace grave, actuelle ou prévisible, une telle conservation est possible, à condition qu'elle soit limitée à une période strictement nécessaire, bien que renouvelable. De plus, dans un objectif de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique, une conservation ciblée et une conservation rapide sont possibles. Ces ingérences nécessitent néanmoins la mise en place de garanties effectives, et d'un contrôle par un juge ou par une autorité administrative indépendante dotée de pouvoirs contraignants.

SOURCES :

MILCHIOR (R.), « La Cour de Justice limite les possibilités de collecter et conserver les données obtenues dans le cadre des communications électroniques », *RLDI*, n°175, Novembre 2020, pp. 27-30

AZOULAY (W.), « Collecte de données électroniques et droits fondamentaux : la CJUE en quête d'équilibre ? », *Lexbase Pénal*, n°32, Novembre 2020, pp. 29-31

NOTE :

L'applicabilité de la directive 2002/58 aux mesures en cause

En vertu de l'article 4 §2 du TUE, les gouvernements font valoir que les mesures critiquées relèvent de leurs fonctions essentielles en ce qu'elles ont pour finalité la sauvegarde de la sécurité nationale, et seraient donc de leur seule compétence, rejetant une application de l'article 15 §1 de la directive 2002/58 dite « vie privée et communications électroniques ». En effet, l'article 1er §3 de celle-ci exclut notamment de son champ d'application les activités régissant la sûreté des États. L'article 15 §1 quant à lui prévoit que les États puissent adopter des mesures visant à limiter les droits prévus par la directive, notamment en matière de confidentialité des communications électroniques. La CJUE énonce alors, contrairement à ce qui est affirmé par les gouvernements, qu'il faut différencier les activités des État visées par l'article 1er §3, qui concerne leurs activités *stricto sensu*, des mesures qu'ils enjoignent aux fournisseurs d'accès, visées par l'article 15 §1. En effet, ces dernières sont effectuées par des opérateurs privées. Elle relèvent donc de la directive 2002/58, quand bien même elles ont été prises à des fins de sécurité nationale. Elles sont donc subordonnées au respect des conditions établies par l'article 15 §1.

Une interdiction des mesures de conservation trop générales contraires au principe de proportionnalité

La CJUE rappelle qu'en vertu de la directive 2002/58, si la confidentialité des communications électroniques est le principe, les ingérences qui y sont portées doivent demeurer des exceptions. L'article 15§1 permet ainsi l'introduction de telles ingérences par les États, qui doivent cependant constituer des mesures « nécessaires, appropriées et proportionnées au sein d'une société démocratique », notamment dans un but de sauvegarde de la sécurité nationale. Toutefois, les mesures prises en vertu de cet article doivent respecter un principe de proportionnalité entre l'objectif qu'elles poursuivent et les droits fondamentaux des personnes concernées, notamment la protection de la vie privée et la protection des données à caractère personnel, garanties par la Charte des droits fondamentaux de l'Union Européenne. Ainsi, vu la grande quantité de données concernées par les mesures critiquées, et le caractère privé des informations qu'elles sont susceptibles de révéler, il est nécessaire d'établir une conciliation entre ces intérêts divergents. Les mesures prises doivent donc arriver à un nécessaire équilibre entre l'objectif d'intérêt général poursuivi, à savoir la sécurité nationale, et les droits en cause, et doivent présenter des garanties suffisantes. Le droit de l'Union s'oppose donc à des mesures nationales qui imposeraient aux fournisseurs une conservation généralisée et indifférenciée des données de connexion à des fins de luttes contre les infractions en générale ou de sauvegarde de la sécurité nationale.

Une interdiction tempérée par des mesures strictement encadrées

Conformément au contrôle de proportionnalité, des ingérences sont toutefois permises au regard de l'importance de l'objectif poursuivi par les mesures. La conciliation de ces droits concurrents conduit alors la CJUE à établir un cadre strict des mesures pouvant être prises par les États. La Cour distingue alors selon les données concernées, les modalités de leur recueil, et la gravité du motif invoqué. En situation de menace « grave, réelle et actuelle ou prévisible » pour la sécurité nationale, les États peuvent déroger à l'interdiction posée précédemment, pour une durée limitée mais renouvelable si la menace persiste. Dans un objectif de lutte contre la criminalité grave et de prévention de menaces terroristes, une conservation ciblée est possible, ainsi qu'une conservation rapide, pour une durée limitée. Toutefois, ces ingérences devront être contrôlées par un juge ou une autorité administrative indépendante dotée de pouvoirs contraignants, et devront être assorties de garanties effectives. La Cour autorise une conservation généralisée et

indifférenciée des adresses IP pour une durée limitée au strict nécessaire. Enfin, s'agissant des données relatives à l'identité civile, considérant le caractère faible l'ingérence, la CJUE autorise leur conservation généralisée et indifférenciée sans délai.

Amalia GAYDON
Master 2 Droit des Médias Électroniques
AIX-MARSEILLE UNIVERSITE, LID2MS-IREDIC 2020

ARRET :

CJUE (Grande Chambre), C-511/18, C-512/18, C-520/18, 6 octobre 2020

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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, ne s'oppose pas à des mesures législatives

– permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

(…)

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.