Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 123/20
Luxembourg, le 6 octobre 2020

Arrêts dans l'affaire C-623/17 Privacy International et dans les affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a.

Presse et Information

La Cour de justice confirme que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation

En revanche, dans des situations dans lesquelles un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, celui-ci peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant, par des mesures législatives, une conservation généralisée et indifférenciée de ces données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. S'agissant de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, un État membre peut également prévoir la conservation ciblée desdites données ainsi que leur conservation rapide. Une telle ingérence dans les droits fondamentaux doit être assortie de garanties effectives et contrôlée par un juge ou une autorité administrative indépendante. De même, il est loisible à un État membre de procéder à une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication dès lors que la durée de conservation est limitée au strict nécessaire ou encore de procéder à une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, sans que cela soit dans ce dernier cas limité à un délai particulier

***

Ces dernières années, la Cour de justice s'est prononcée, dans plusieurs arrêts, sur la conservation et l'accès aux données à caractère personnel dans le domaine des communications électroniques [1]. La jurisprudence qui en découle, en particulier l'arrêt Tele2 Sverige et Watson e.a., dans lequel elle a notamment considéré que les États membres ne pouvaient pas imposer

[1] Ainsi, dans l'arrêt du 8 avril 2014, Digital Rights Ireland e.a (C-293/12 et C-594/12, EU:C:2014:238) (voir CP n° 54/14), la Cour a déclaré invalide la 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 2006, L 105, p. 54), au motif que l'ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel, reconnus par la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), que comportait l'obligation générale de conservation des données relatives au trafic et à la localisation prévue par cette directive n'était pas limitée au strict nécessaire. Dans l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970) (voir CP n° 145/16), la Cour a ensuite interprété 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 "vie privée et communications électroniques" »). Cet article habilite les États membres – pour des raisons de protection, entre autres, de la sécurité nationale – à adopter des « mesures législatives » afin de limiter la portée de certains droits et obligations prévus par la directive. Enfin, dans l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788) (voir CP n° 141/18), la Cour a interprété ce même article 15, paragraphe 1, dans une affaire qui concernait l'accès des autorités publiques aux données relatives à l'identité civile des utilisateurs des moyens de communications électroniques.

aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, a suscité les préoccupations de certains États, craignant d'avoir été privés d'un instrument qu'ils estiment nécessaire à la sauvegarde de la sécurité nationale et à la lutte contre la criminalité.

C'est sur cette toile de fond que l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) (Privacy International, C-623/17), le Conseil d'État (France) (La Quadrature du Net e.a., affaires jointes C-511/18 et C-512/18) ainsi que la Cour constitutionnelle (Belgique) (Ordre des barreaux francophones et germanophone e.a., C-520/18) ont été saisis de litiges concernant la légalité des réglementations adoptées par certains États membres dans ces domaines, prévoyant en particulier une obligation pour les fournisseurs de services de communications électroniques de transmettre à une autorité publique ou de conserver de manière généralisée ou indifférenciée les données des utilisateurs relatives au trafic et à la localisation.

Par deux arrêts prononcés en grande chambre, le 6 octobre 2020, la Cour juge tout d'abord que la directive « vie privée et communications électroniques » s'applique à des réglementations nationales imposant aux fournisseurs de services de communications électroniques de procéder, aux fins de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, à des traitements de données à caractère personnel, tels que leur transmission à des autorités publiques ou leur conservation. En outre, tout en confirmant sa jurisprudence issue de l'arrêt Tele2 Sverige et Watson e.a., sur le caractère disproportionné d'une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, la Cour **apporte des précisions**, notamment, quant à **l'étendue des pouvoirs** que reconnaît cette directive aux États membres en matière de conservation de telles données aux fins précitées.

Tout d'abord, la Cour prend soin de dissiper les doutes sur l'applicabilité de la directive « vie privée et communications électroniques » soulevés dans le cadre des présentes affaires. En effet, plusieurs États membres ayant soumis des observations écrites à la Cour ont exprimé un avis divergent à cet égard. Ils faisaient notamment valoir que cette directive ne trouverait pas à s'appliquer aux réglementations nationales en cause, dans la mesure où celles-ci ont pour finalité la sauvegarde de la sécurité nationale, qui relèverait de leur seule compétence, comme en témoignerait notamment l'article 4, paragraphe 2, troisième phrase, TUE. La Cour considère cependant que **des réglementations nationales imposant aux fournisseurs de services de communications électroniques de conserver des données relatives au trafic et à la localisation ou encore de transmettre ces données aux autorités nationales de sécurité et de renseignement à cette fin relèvent du champ d'application de la directive**.

Ensuite, la Cour rappelle que la « directive vie privée et communications électroniques » [2] ne permet pas que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et à l'interdiction de stocker ces données devienne la règle. Ceci implique que cette directive **n'autorise les États membres à adopter, entre autres à des fins de sécurité nationale, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic [3], que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte** [4].

Dans ce cadre, la Cour considère, d'une part, dans l'affaire Privacy International, que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, **s'oppose à une réglementation nationale, imposant aux fournisseurs de services de communications électroniques, en vue de la sauvegarde de la sécurité nationale, la transmission généralisée et indifférenciée aux services de sécurité et de renseignement des données relatives au trafic et à la localisation**. D'autre part, dans les affaires jointes La Quadrature du Net e.a., ainsi

[2] Article 15, paragraphes 1 et 3, de la directive 2002/58.

[3] Article 5, paragraphe 1, de la directive 2002/58.

[4] En particulier, les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la Charte.

que dans l'affaire Ordre des barreaux francophones et germanophone e.a., la Cour estime que cette même directive **s'oppose à des mesures législatives imposant aux fournisseurs de services de communications électroniques, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation**. En effet, ces obligations de transmission et de conservation généralisée et indifférenciée de telles données constituent des **ingérences particulièrement graves dans les droits fondamentaux garantis par la Charte**, sans que le comportement des personnes dont les données sont concernées présente de lien avec l'objectif poursuivi par la réglementation en cause. De manière analogue, la Cour interprète l'article 23, paragraphe 1, du règlement général sur la protection des données [5], lu à la lumière de la Charte, en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

En revanche, la Cour estime que, **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 directive « vie privée et communications électroniques », lue à la lumière de la Charte, **ne s'oppose pas au fait d'enjoindre aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation**. Dans ce contexte, la Cour précise que la décision prévoyant cette injonction, pour une période temporellement limitée au strict nécessaire, doit 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, afin de vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties prévues. Dans ces mêmes conditions, ladite directive ne s'oppose pas non plus à l'analyse automatisée des données, notamment celles relatives au trafic et à la localisation, de l'ensemble des utilisateurs de moyens de communications électroniques.

La Cour ajoute que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas à des mesures législatives permettant le recours à une **conservation ciblée, temporellement limitée au strict nécessaire, des données relatives au trafic et à la 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**. De même, cette directive ne s'oppose pas à de telles mesures prévoyant une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication, pour autant que la durée de conservation est **limitée au strict nécessaire**, ni à celles prévoyant une telle conservation des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, les États membres n'étant dans ce dernier cas pas tenus de limiter temporellement la conservation. Au surplus, ladite directive ne s'oppose pas à une mesure législative permettant le recours à une conservation rapide des données dont disposent les fournisseurs de services dès lors que se présentent des **situations dans lesquelles survient la nécessité de conserver lesdites données au-delà des délais légaux de conservation des données aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale**, lorsque ces infractions ou atteintes ont déjà été constatées ou lorsque leur existence peut être raisonnablement soupçonnée.

En outre, la Cour juge que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, **ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir au recueil en temps réel**, notamment, **des données relatives au trafic et à la localisation**, lorsque ce recueil est **limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées**, d'une manière ou d'une autre, **dans des activités de terrorisme** et est soumis à un **contrôle préalable, effectué soit par une juridiction, soit par une entité**

[5] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1).

administrative indépendante, dont la décision est dotée d'un effet contraignant, s'assurant qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence, le contrôle doit intervenir dans de brefs délais.

Enfin, la Cour aborde la question du maintien des effets dans le temps d'une réglementation nationale jugée incompatible avec le droit de l'Union. À cet égard, elle juge qu'une juridiction nationale **ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, à l'égard d'une réglementation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, jugée incompatible avec la directive « vie privée et communications électroniques »**, lue à la lumière de la Charte.

Ceci étant dit, afin de donner une réponse utile à la juridiction nationale, la Cour rappelle que **l'admissibilité et l'appréciation d'éléments de preuve qui ont été obtenus par une conservation de données contraire au droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, relève, en l'état actuel du droit de l'Union, du seul droit national**. Toutefois, la Cour précise que la directive « vie privée et communications électroniques », interprétée à la lumière du principe d'effectivité, exige que le juge pénal national **écarte des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation incompatible avec le droit de l'Union**, dans le cadre d'une telle procédure pénale, si les personnes soupçonnées d'actes de criminalité ne sont pas en mesure de prendre efficacement position sur ces éléments de preuve.

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 : Amanda Nouvel ☎ (+352) 4303 2524.