Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 4/20
Luxembourg, le 15 janvier 2020

Presse et Information

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

Avocat général Campos Sánchez-Bordona : les moyens et les méthodes de la lutte antiterroriste doivent répondre aux exigences de l'État de droit

La directive vie privée et communications électroniques s'applique, en principe, lorsque les fournisseurs de services de communications électroniques sont obligés, par la loi, de conserver les données de leurs abonnés et de permettre aux autorités publiques d'y accéder, indépendamment du fait que ces obligations s'imposent pour des raisons de sécurité nationale

Ces dernières années, la Cour de justice s'est prononcée, dans plusieurs arrêts, sur la conservation et l'accès aux données à caractère personnel [1]. La jurisprudence qui en découle, en particulier l'arrêt Tele2 Sverige et Watson e.a., dans lequel elle a déclaré que les États membres ne pouvaient pas imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée, préoccupe certains États, qui se sentent privés d'un instrument qu'ils estiment nécessaire à la sauvegarde de la sécurité nationale et à la lutte contre la criminalité et le terrorisme.

Cette préoccupation a été exprimée dans **quatre renvois préjudiciels**, présentés respectivement par le Conseil d'État (France) (affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a.), la Cour constitutionnelle (Belgique) (C-520/18, Ordre des barreaux francophones et germanophone e.a.) et l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) (C-623/17, Privacy International). **Ces renvois soulèvent, tout d'abord, le problème de l'application de la directive à des activités liées à la sécurité nationale et à la lutte contre le terrorisme.**

Dans ses conclusions présentées ce jour sur ces renvois préjudiciels, **l'avocat général Manuel Campos Sánchez-Bordona dissipe, en premier lieu, les doutes sur l'applicabilité de la directive.** Il précise que la **directive exclut** de son application **les activités menées, en vue de préserver la sécurité nationale, par les pouvoirs publics pour leur propre compte, sans requérir la collaboration de particuliers et, dès lors, sans leur imposer d'obligations dans leur gestion commerciale**. En revanche, **lorsque le concours de particuliers auxquels certaines obligations sont imposées est requis, même pour des raisons de sécurité nationale, cette circonstance relève du domaine régi par le droit de l'Union, celui de la protection de la vie privée qui peut être exigée de ces acteurs privés**. Ainsi, **la directive**

[1] Arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland e.a. (voir CP n° 54/14), dans lequel la Cour a déclaré l'invalidité de 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). Elle a considéré que la directive permettait une ingérence disproportionnée dans les droits au respect de la vie privée et familiale et à la protection des données à caractère personnel, reconnus par la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »). Arrêt du 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15, Tele2 Sverige et Watson e.a. (voir CP nº 145/16), dans lequel la Cour a 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) (ci-après la « directive »). Cet article habilitait 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. Arrêt du 2 octobre 2018, C-207/16, Ministerio Fiscal (voir CP n° 141/18), dans lequel la Cour a confirmé l'interprétation précitée.

s'applique, en principe, lorsque les fournisseurs de services de communications électroniques sont tenus, par la loi, de conserver les données de leurs abonnés et de permettre aux autorités publiques d'y accéder, comme dans les affaires examinées, **indépendamment du fait que ces obligations soient imposées aux fournisseurs pour des raisons de sécurité nationale**.

Par ailleurs, la directive permet aux États membres de prendre des mesures légales qui, à des fins de sécurité nationale, **concernent les activités des personnes** soumises à l'imperium des États membres, **en limitant leurs droits**. L'avocat général rappelle que les **limitations posées à l'obligation de garantir la confidentialité des communications et des données relatives au trafic y afférentes doivent être interprétées strictement et à la lumière des droits fondamentaux consacrés par la Charte**.

M. Campos Sánchez-Bordona propose de confirmer la jurisprudence de la Cour issue de l'arrêt Tele2 Sverige et Watson e.a. en insistant sur le caractère disproportionné d'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. Toutefois, il reconnaît l'utilité d'une obligation de conservation des données pour sauvegarder la sécurité nationale et lutter contre la criminalité. C'est pourquoi il plaide en faveur d'une **conservation limitée et différenciée** (c'est-à-dire la conservation de certaines catégories de données absolument indispensables pour la prévention et le contrôle efficaces de la criminalité et pour la sauvegarde de la sécurité nationale durant une période déterminée et différenciée en fonction de chaque catégorie), ainsi que pour **un accès limité à ces données** (soumis à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, à l'information des personnes concernées, pour autant que cela ne compromette pas les enquêtes en cours, et à l'adoption de règles visant à prévenir toute utilisation abusive et tout accès illicite aux données). Il ajoute, toutefois, que rien ne s'oppose à ce que, dans des situations réellement exceptionnelles caractérisées par une menace imminente ou par un risque extraordinaire justifiant la constatation officielle de la situation d'urgence, la législation nationale prévoie, pour une durée limitée et avec les garanties juridictionnelles correspondantes, la possibilité d'imposer une obligation de conservation des données aussi étendue et générale qu'il est jugé indispensable.

En réponse à la première question soulevée par le Conseil d'État, l'avocat général déclare que la **directive s'oppose à la réglementation française qui, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, impose aux opérateurs et aux prestataires de services de communications électroniques de conserver, de manière générale et indifférenciée, les données relatives au trafic et les données de localisation de tous les abonnés ainsi que les données permettant d'identifier les créateurs de contenus offerts par les fournisseurs de ces services.** Il souligne que, comme le reconnaît le Conseil d'État lui-même, **l'obligation de conservation imposée par la réglementation française est généralisée et indifférenciée, de sorte qu'elle constitue une ingérence particulièrement grave dans les droits fondamentaux consacrés par la Charte.** De même, il rappelle que, dans l'arrêt Tele2 Sverige et Watson e.a., **la Cour a rejeté la possibilité d'une conservation de ces données en lien avec la lutte contre le terrorisme**. L'avocat général soutient que la lutte antiterroriste ne doit pas être envisagée uniquement en termes d'*efficacité pratique* mais aussi en termes d'*efficacité juridique* afin que ses moyens et ses méthodes répondent aux exigences du respect de l'État de droit, qui soumet le pouvoir et la force aux limites du droit et, en particulier, à un ordre juridique dont la défense des droits fondamentaux constitue la raison d'être et la finalité. Par ailleurs, **la réglementation française n'est pas non plus compatible avec la directive car elle n'instaure pas l'obligation d'informer les personnes concernées du traitement de leurs données à caractère personnel effectué par les autorités compétentes,** afin que ces personnes puissent exercer leur droit à une protection juridictionnelle effective, **pour autant que cette communication ne compromette pas l'action de ces autorités**.

En revanche, **la directive ne s'oppose pas à une réglementation nationale qui permet de recueillir, en temps réel, les données relatives au trafic et les données de localisation de personnes spécifiques, pour autant que ces actions soient menées conformément aux**

procédures prévues pour l'accès aux données à caractère personnel légalement conservées et avec les mêmes garanties.

Dans l'affaire C-520/18, l'avocat général suggère à la Cour de répondre à la Cour constitutionnelle que la directive **s'oppose à** une **réglementation** qui, comme la réglementation **belge**, a pour objectif non seulement la lutte contre le terrorisme et les formes de criminalité les plus graves, mais aussi la défense du territoire, la sécurité publique, la recherche, la découverte et la poursuite d'autres délits que ceux de criminalité grave, et, d'une manière générale, tout autre objectif prévu à l'article 23, paragraphe 1, du règlement 2016/679 [2]. La raison en est que, **même si l'accès aux données conservées est soumis à des garanties précisément réglementées**, **les opérateurs et les fournisseurs de services de communications électroniques se voient imposer, dans ce cas également, une obligation générale et indifférenciée** qui s'applique de manière permanente et continue, de conserver les données relatives au trafic et les données de localisation traitées dans le cadre de la fourniture de ces services, ce qui est incompatible avec la Charte.

Concernant la question de savoir si, dans l'hypothèse où la réglementation nationale serait incompatible avec le droit de l'Union, ses effets pourraient être provisoirement maintenus, l'avocat général considère qu'**une juridiction nationale peut, si le droit interne le permet, maintenir, exceptionnellement et provisoirement, les effets d'une législation, telle que la réglementation belge, même si elle est incompatible avec le droit de l'Union, si ce maintien est justifié par des considérations impérieuses liées à des menaces pour la sécurité publique ou nationale auxquelles d'autres moyens ou solutions de substitution ne permettraient pas de parer. Ce maintien ne peut durer que le temps strictement nécessaire pour remédier à l'incompatibilité susvisée.**

Enfin, dans l'affaire C-623/17, il convient de déterminer si une réglementation nationale imposant à un fournisseur de services de communications électroniques l'obligation de fournir aux **services de sécurité et de renseignement du Royaume-Uni** (United Kingdom Security and Intelligence Agencies) **des données de communications en masse** après leur collecte généralisée et indifférenciée est compatible avec la directive. L'avocat général estime que, **nonobstant l'article 4 TUE, selon lequel la sécurité nationale relève de la responsabilité exclusive de chaque État membre, la directive s'oppose à la réglementation britannique.**

RAPPEL : Les conclusions de l'avocat général ne lient pas la Cour de justice. La mission des avocats généraux consiste à proposer à la Cour, en toute indépendance, une solution juridique dans l'affaire dont ils sont chargés. Les juges de la Cour commencent, à présent, à délibérer dans cette affaire. L'arrêt sera rendu à une date ultérieure.

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 : Antoine Briand ☎ (+352) 4303 3205.

Des images de la lecture des conclusions sont disponibles sur « Europe by Satellite » ☎ (+32) 2 2964106.

[2] 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).