Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 59/18
Luxembourg, le 3 mai 2018

Presse et Information

Conclusions de l'avocat général dans l'affaire C-207/16
Ministerio Fiscal

L'avocat général Saugmandsgaard Øe propose à la Cour de déclarer que même les infractions pénales qui ne sont pas d'une particulière gravité peuvent justifier un accès aux métadonnées de base des communications électroniques pourvu que cet accès ne porte pas une atteinte grave à la vie privée

Dans le cadre de l'enquête d'un vol avec violences d'un portefeuille et d'un téléphone mobile, la police judiciaire espagnole a demandé au juge d'instruction de lui accorder l'accès aux données d'identification des utilisateurs des numéros de téléphone activés depuis le téléphone volé durant une période de douze jours à partir de la date du vol. Le juge d'instruction a rejeté cette demande, au motif notamment que les faits à l'origine de l'enquête pénale n'auraient pas été constitutifs d'une infraction « grave » – c'est-à-dire, selon le droit espagnol, une infraction sanctionnée d'une peine de prison supérieure à cinq ans –, l'accès aux données d'identification n'étant en effet possible en Espagne que pour ce type d'infractions. Le Ministerio Fiscal (ministère public espagnol) a interjeté appel de cette décision devant l'Audiencia Provincial de Tarragona (cour provinciale de Tarragone, Espagne).

La directive vie privée et communications électroniques [1] prévoit que les États membres peuvent restreindre les droits des citoyens lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques.

Dans ses arrêts Digital Rights [2] et Tele2 Sverige [3], la Cour de justice a utilisé la notion d'« infractions graves » pour apprécier la légitimité et la proportionnalité d'une ingérence dans le droit au respect de la vie privée et familiale ainsi que dans le droit à la protection des données à caractère personnel, ces deux droits étant consacrés dans la charte des droits fondamentaux de l'Union européenne.

[1] 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).

[2] Arrêt du 8 avril 2014, Digital Rights Ireland (C-293/12 et C-594/12, voir CP nº 54/14). Dans cet arrêt, 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).

[3] Arrêt du 21 décembre 2016, Tele2 Sverige (C-203/15 et C-698/15, voir CP nº 145/16). Dans cet arrêt, la Cour a jugé que le droit de l'Union s'oppose, *d'une part*, « à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, 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, *d'autre part*, « à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union ».

L'Audiencia Provincial de Tarragona indique que, après l'adoption de la décision du juge d'instruction, le législateur espagnol a introduit deux critères alternatifs pour déterminer le degré de gravité d'une infraction à l'égard de laquelle la conservation et la communication des données personnelles sont autorisées. Le premier est un critère matériel, attaché au terrorisme et aux infractions commises dans le cadre d'une organisation criminelle. Le second est un critère normatif formel, qui fixe un seuil minimal de trois ans d'emprisonnement. La juridiction espagnole souligne que ce seuil pourrait englober la grande majorité des qualifications pénales. L'Audiencia Provincial de Tarragona interroge donc la Cour sur la fixation du seuil de gravité des infractions à partir duquel une atteinte aux droits fondamentaux peut être justifiée, au regard des arrêts précités, lors de l'accès, par les autorités nationales compétentes, aux données à caractère personnel conservées par les fournisseurs de services de communications électroniques.

Dans ses conclusions de ce jour, l'avocat général Henrik Saugmandsgaard Øe constate tout d'abord qu'une mesure telle que celle demandée par la police judiciaire en l'espèce est constitutive d'une ingérence dans le droit au respect de la vie privée et familiale ainsi que dans le droit à la protection des données à caractère personnel. Cependant, l'avocat général estime que, **dans les arrêts Digital Rights et Tele2, la Cour a établi un lien de corrélation entre la gravité de l'ingérence constatée et la gravité du motif permettant de justifier celle-ci**. Ainsi, pour exiger, au stade de la justification d'une telle ingérence, qu'il existe une « infraction grave » permettant de déroger au principe de confidentialité des communications électroniques, il faut que **l'ingérence soit grave**. **Selon l'avocat général, cet élément essentiel fait défaut en l'espèce**.

L'avocat général ajoute que la nature de l'ingérence en cause dans cette affaire est distincte des ingérences envisagées dans les deux arrêts précités. **Il s'agit en effet d'une mesure ciblée** qui tend à une possibilité d'accès, par les autorités compétentes et pour les besoins d'une enquête pénale, à des données détenues à des fins commerciales par des prestataires de service et qui porte uniquement sur l'identité (nom, prénom et éventuellement adresse) d'une catégorie restreinte d'abonnés ou d'utilisateurs d'un moyen de communication spécifique, à savoir ceux dont le numéro de téléphone a été activé depuis le téléphone mobile dont le vol fait l'objet de l'enquête, **et ce durant une période limitée**, à savoir une douzaine de jours. **L'avocat général considère que les effets potentiellement nuisibles, pour les personnes visées par la demande d'accès en cause, sont à la fois modérés et encadrés**, étant donné que les données demandées ne sont pas destinées à être divulguées au grand public et que la faculté d'accès offerte aux autorités policières est entourée de garanties procédurales, puisqu'elle donne lieu à un contrôle juridictionnel. **Par conséquent, l'ingérence entraînée par la communication de ces données d'identité civile ne revêt pas un caractère de particulière gravité**, dès lors que, dans ces circonstances particulières, de telles données n'affectent pas directement et fortement l'intimité de la vie privée des personnes concernées.

L'avocat général indique que, selon la directive, une dérogation au principe de confidentialité des communications électroniques peut être justifiée par l'objectif d'intérêt général de prévenir et poursuivre des *infractions pénales*, sans autre précision quant à la nature de celles-ci. Il n'est donc pas impératif que les infractions légitimant la mesure restrictive en cause puissent être qualifiées de « graves » au sens des arrêts Digital Rights et Tele2. Selon l'avocat général, **c'est uniquement lorsque l'ingérence subie est d'une particulière gravité que les infractions susceptibles de justifier une telle ingérence doivent elles-mêmes être d'une particulière gravité. En revanche, dans le cas d'une ingérence non grave (c'est-à-dire quand les données dont la communication est demandée ne portent pas une atteinte grave à la vie privée), même les infractions pénales qui ne sont pas d'une particulière gravité sont susceptibles de justifier une telle ingérence (à savoir l'accès aux données demandées).**

En particulier, l'avocat général estime que **le droit de l'Union ne s'oppose pas à ce que les autorités compétentes puissent avoir accès aux données d'identification détenues par les fournisseurs de services de communications électroniques, lorsque ces données permettent de retrouver les auteurs supposés d'une infraction pénale ne revêtant pas de caractère grave**. **L'avocat général en conclut que, à la lumière de la directive, la mesure demandée par la police judiciaire en l'espèce entraîne, dans les droits fondamentaux garantis par la directive et par la Charte, une ingérence qui n'atteint pas un niveau de**

gravité suffisant pour qu'il faille réserver un tel accès aux cas dans lesquels l'infraction concernée revêt un caractère grave.

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 : Gilles Despeux ☎ (+352) 4303 3205.