Arrêt de la Cour
Affaire C-207/16 *Ministerio Fiscal* du 2 octobre 2018

DATE 22-10-2018

ÉMETTEUR BAJ

Dans un arrêt du 2 octobre 2018, la Cour de Justice de l'Union Européenne a reconnu que les infractions pénales sans particulière gravité peuvent justifier un accès aux données personnelles conservées par les fournisseurs de services de communications électroniques lorsqu'un tel accès ne porte pas une atteinte injustifiée à la vie privée.

Après une présentation des faits, de la procédure et des questions préjudicielles (I), il conviendra d'analyser la décision de la Cour (II).

1 | Les faits et la procédure

Dans le cadre du traitement d'une plainte d'un ressortissant espagnol victime du vol avec violence de son téléphone portable et afin de retrouver le coupable, la police judiciaire a saisi le juge d'instruction d'une demande tendant à ordonner aux opérateurs de téléphonie :

- d'une part, la transmission des numéros de téléphone activés à compter du vol (et pendant 12 jours) avec le code IMEI relatif à l'identité internationale d'équipement mobile du téléphone volé ;
- d'autre part, les données relatives à l'identité (noms, prénoms, adresse) des titulaires ou utilisateurs des numéros de téléphones correspondant aux cartes SIM téléphoniques activées avec le code IMEI.

Par une ordonnance du 5 mai 2015, le juge d'instruction a rejeté cette demande au motif que les faits à l'origine de l'enquête n'étaient pas constitutifs d'une infraction grave au sens de la législation nationale en vigueur qui limitait la conservation des données aux infractions graves punies de peines d'emprisonnement supérieures à 5 ans et ne pouvaient donc pas justifier l'accès aux données demandées.

Le ministère public espagnol – seule partie à la procédure – a interjeté appel devant la Cour provinciale de Tarragone en s'appuyant sur un arrêt de la Cour suprême espagnole qui avait accordé la communication des données dans une affaire où les faits étaient similaires[1].

La juridiction d'appel a ordonné à titre conservatoire aux opérateurs de téléphonie la prolongation de la conservation des données concernées en l'espèce.

[1] Arrêt de la chambre pénale de la Cour Suprême, 26 juillet 2010 n°745/2010, ES:TS:2010:4200

Postérieurement à l'ordonnance prononcée par le juge d'instruction, le législateur espagnol a modifié le code de procédure pénale[2] et y a introduit deux critères alternatifs permettant d'apprécier la gravité d'une infraction et de déterminer si la conservation et la communication des données personnelles sont autorisées :

- un critère matériel fondé sur le caractère spécifique et grave des infractions pénales qui sont particulièrement préjudiciables aux intérêts juridiques individuels et collectifs ;
- un critère normatif formel fondé sur la peine prévue pour l'infraction en cause avec un seuil fixé à 3 ans d'emprisonnement, couvrant ainsi une majorité d'infractions.

Les nouvelles dispositions modifiant le code de procédure pénale réduisent considérablement le seuil de gravité des infractions à l'égard desquelles sont autorisées la conservation et la communication de données personnelles. Toutefois, la juridiction d'appel, s'interrogeant sur les éléments à prendre en compte pour déterminer dans quelle mesure la gravité d'une infraction est suffisante pour justifier l'ingérence dans les droits fondamentaux à la suite de l'arrêt de la CJUE *Digital Rights,*[3] a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

- *« Est-il possible de déterminer la gravité suffisante des infractions, en tant que critère justifiant l'atteinte aux droits fondamentaux reconnus aux articles 7 et 8 de la [Charte], uniquement en prenant en considération la peine dont peut être punie l'infraction faisant l'objet d'une enquête ou est-il nécessaire, en outre, d'identifier dans les comportements délictueux un caractère préjudiciable particulier pour des intérêts juridiques individuels ou collectifs ?*

- *Le cas échéant, s'il était conforme aux principes fondamentaux de l'Union appliqués par la Cour dans son arrêt [du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238] en tant que normes de contrôle strict de la directive [2002/58], de déterminer la gravité de l'infraction uniquement en fonction de la peine susceptible d'être infligée, quel devrait être le niveau minimal de cette peine ? Un niveau fixé de manière générale à un minimum de trois ans serait-il conforme ? »*

Le président de la CJUE a suspendu la procédure en attendant le prononcé de l'arrêt des affaires jointes *Tele2 Sverige et Watson*[4] aux fins de savoir si la juridiction de renvoi espagnole souhaiterait maintenir sa demande de question préjudicielle.

Après le prononcé de l'arrêt le 21 décembre 2016, la Cour provinciale de Tarragone a souhaité maintenir sa demande de question préjudicielle au motif que l'arrêt Tele2 ne définissait pas clairement la notion de gravité de l'infraction servant à apprécier le caractère justifié d'une mesure d'ingérence et par conséquent d'apprécier la règlementation nationale en cause. La procédure devant la CJUE a repris le 16 février 2017.

[2] Loi organique 13/2015
[3] Arrêt du 8 avril 2014, *Digital Rights*, C-293/12 et C-594/12, EU:C:2014:238 dans lequel la Cour a constaté que la directive 2006/24 permettant la conservation et la communication des données relatives au trafic constituent une ingérence particulièrement grave dans les droits fondamentaux. La Cour a ainsi précisé que toute limitation doit être prévue par la loi, respecter les droits et libertés et respecter le principe de proportionnalité. Pour procéder au contrôle du respect du principe de proportionnalité, la Cour a dégagé des critères.
[4] Arrêt du 21 décembre 2016,Tele2 Sverige et Watson e.a., C-203/15 et C-698/15

2 | Le raisonnement de la CJUE

2.1 Reformulation de la première question préjudicielle : examen préalable de la gravité de l'ingérence avant l'appréciation de la gravité de l'infraction

La première question posée par la juridiction de renvoi s'inscrit dans la continuité de l'arrêt *Digital Rights*[5] qui employait la notion « d'infraction grave » ou de « criminalité grave » en tant que critère de vérification de la finalité et de proportionnalité de l'ingérence dans les droits fondamentaux. Il est demandé à la CJUE de définir les éléments à prendre en compte pour établir quand la gravité d'une infraction pénale justifie que soit porté atteinte aux droits fondamentaux dans le cadre de la conservation et de l'accès aux données personnelles.

L'avocat général estime qu'avant que la Cour ne se prononce sur cette question, il faut examiner au préalable si l'ingérence en cause présente un degré de gravité suffisamment élevé pour qu'il soit exigé que cette ingérence soit justifiée par la lutte contre une infraction à caractère grave afin de pouvoir être admise.

Il en conclut que la reformulation de la première question est nécessaire pour que la réponse de la CJUE porte sur l'interprétation de l'article 15 (1) de la directive 2002/58[6] dans le cas d'espèce, à savoir une ingérence sans particulière gravité dont l'objet est la lutte contre une infraction pénale dont le caractère grave est mis en doute.

La CJUE ayant suivi le raisonnement de l'avocat général, elle n'a traité que la première question préjudicielle sous l'angle de la gravité de l'ingérence.

En d'autres termes, la cour a ainsi confirmé qu'il ne s'agit ni d'appréhender les législations pénales de manière générale et absolue ni de réserver les cas de conservation à des catégories limitatives d'infractions pénales. L'enjeu est de faire une stricte application du principe de proportionnalité pour juger du caractère légitime ou non des atteintes aux droits fondamentaux et pour cela de mettre en balance au cas par cas le but poursuivi par la disposition en cause et les moyens mis en œuvre pour y parvenir.

C'est pour cette raison que la Cour a dégagé ce nouveau critère de « gravité de l'ingérence » afin de moduler les atteintes aux droit fondamentaux au regard du but poursuivi. Ainsi, l'ingérence est possible pour une infraction mineure mais doit rester de faible proportion pour être légitime. Inversement, plus l'infraction sera lourde et plus l'ingérence pourra retenir une certaine gravité.

2.2 La gravité de l'ingérence, critère déterminant les conditions d'accès aux données conservées par les fournisseurs de services de communications électroniques par les autorités publiques

a) L'arrêt *Ministerio Fiscal* : cas d'ingérence sans particulière gravité tend à viser les « infractions pénales » en général et non pas seulement les infractions « graves »

Les conclusions de l'avocat général dans l'arrêt *Ministerio Fiscal* rappellent que l'accès des autorités publiques aux données personnelles conservées par les opérateurs de téléphonie constitue une ingérence dans le droit au respect de la vie privée[7] quelles que soient les données personnelles concernées, qu'il s'agisse de données sensibles ou non ou que les personnes concernées aient subi ou non des inconvénients suite à ladite ingérence.

[5] Comme le relève l'avocat général, la notion d' « infractions graves » a été employée dans l'arrêt *Digital Rights* en tant que critère de vérification de la finalité et de la proportionnalité de l'ingérence dans les droits fondamentaux.
[6] 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)
[7] Article 7 de la charte des droits fondamentaux de l'Union Européenne

L'article 15 (1) de la directive 2002/58 énumère de manière exhaustive les objectifs permettant à une règlementation nationale de déroger au principe de confidentialité des communications électroniques en donnant accès aux autorités publiques aux données conservées par les fournisseurs de services de communications électroniques.

L'accès doit par conséquent répondre « *effectivement et strictement* » à l'un des objectifs listé à l'article 15 (1) : « *lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — 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* ».

La Cour indique que l'objectif de prévention, de recherche, de détection et de poursuite de l'article 15 (1) vise les « *infractions pénales* » en général et non pas seulement les infractions « graves ».

En l'espèce, le contrôle de proportionnalité opéré par la Cour implique un examen des circonstances de temps et de lieu afin d'apprécier le caractère circonscrit ou non de l'atteinte aux droits fondamentaux au regard du but poursuivi.

Le but : Il s'agissait d'un vol de téléphone portable et donc du traitement d'une « infraction pénale » au sens général. La demande d'accès aux données conservées par les FAI apparait dès lors, pour la Cour, justifiée.

Pour la durée de conservation : la Cour rappelle que la police judiciaire ne souhaitait accéder qu'aux données permettant uniquement de mettre en relation les cartes SIM activées – ainsi que leurs titulaires – avec le téléphone volé pour une période réduite de 12 jours.

Pour le ciblage de la mesure et de ses effets pour les personnes : les personnes concernées sont clairement définies puisqu'il ne peut s'agir que de celles ayant utilisé le téléphone portable après sa soustraction à la victime. La CJUE estime que ces données ciblées et déterminées quant à la durée « *ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées* »[8].

La CJUE conclut que l'accès aux données demandé par la police judiciaire « *comporte une ingérence dans les droits fondamentaux […] qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave* ».

b) La notion d'ingérence grave tend à viser les cas d'infractions graves

Comme le rappelle l'avocat général faisant référence à l'arrêt Tele2 dans ses conclusions dans l'arrêt *Ministerio Fiscal*, « *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* »[9].

Dans l'affaire Tele2, pour lutter contre la criminalité, les règlementations nationales en cause prévoyaient la conservation généralisée des données relatives au trafic et aux données de localisation.

La Cour pouvait donc légitimement estimer que l'accès des autorités publiques aux données à caractère personnel conservées par les FAI ne pouvait être justifié qu'en matière lutte contre la criminalité grave, dans la mesure où, « *prises dans leur ensemble, ces données [étaient] susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées* »[10].

[8] Paragraphe 60 de l'arrêt
[9] Paragraphe 89 des conclusions de l'avocat général dans l'arrêt *Ministerio Fiscal*
[10] Paragraphe 99 de l'arrêt