RÉTENTION DE DONNÉES : ENTRE ANNULATION D'UNE DIRECTIVE EXCESSIVE ET MODE D'EMPLOI À DESTINATION DE LA COMMISSION

CJUE, 8 avril 2014, Digital Rights Ireland Ltd & Kärntner Landesregierung

DATA RETENTION: A STRUCK DOWN DIRECTIVE AND AN INSTRUCTION MANUAL TO AVOID MASS SURVEILLANCE

Par **Pierre DESMARAIS***

RÉSUMÉ

Après des années de contentieux, tant contre la directive que ses mesures de transposition en droit national, la Cour de Justice de l'Union Européenne a annulé la directive *Rétention de données* (n° 2006/24), le 8 avril dernier. Mais si les juges ont considéré que le législateur communautaire avait commis une ingérence disproportionnée dans les droits au respect de la vie privée et à la protection des données personnelles, ils n'ont pas pour autant condamné le principe de la conservation des *données de connexion* lorsque cela s'avère ou serait susceptible de s'avérer nécessaire à la lutte contre la criminalité. Plus que comme une sanction, la décision doit donc être considérée comme un *mode d'emploi* dans la création de traitements de données de masse.

MOTS-CLÉS

Donnée de connexion, Rétention, Crime, Vie privée, Protection des données.

SUMMARY

After years of litigation, both against the directive and its national transposition measures, the European Court offustice stroke down the Data Retention Directive (No. 2006/24), on 8 April 2014. But if the judges considered that the EU directive was construed as disproportionate interference with the right to privacy and to the protection of personal data, they nonetheless did not condemn the principle of retention of data connection provided this is or islikely to be necessary in the fight against crime. More than a sanction, this case should be regarded as a "How to create mass data processing".

KEYWORDS

Connection data, Retention, Crime, Privacy, Data protection.

* Avocat à la Cour – CIL, pierre@desmarais-avocats.fr

La défense des droits fondamentaux constitue un principe fondateur de l'Union et une condition indispensable de sa légitimité ».

Peut-être les rédacteurs de la directive n° 2006/24 du 15 mars 2006 auraient-ils dû relire cette phrase extraite des conclusions du Conseil Européen de Cologne avant de prendre la plume. Car le 8 avril 2014, deux arrêts de la Cour de Justice de l'Union Européenne (CJUE) sonnaient le glas de cette directive. Le combat aura néanmoins été âpre. Il aura fallu plusieurs dizaines d'arrêts de la Cour pour aboutir à ce que d'aucuns considéraient comme inévitable.

A l'origine de ces deux décisions, des citoyens, les Etats membres ayant échoué. La première question préjudicielle émanait de la *High Court* irlandaise, saisie d'un litige contre la mesure de transposition par la société *Digital Rights Ireland* « *ayant pour objet statutaire la promotion et la protection des droits civiques et des droits de l'homme, en particulier dans l'univers des technologies de communication modernes* » (1). La seconde question préjudicielle a été déposée par le Verfassungsgerichtshof autrichien dans le cadre d'une instance introduite par un *Land* et pas moins de 11 000 personnes physiques. Les questions posées par les deux juridictions étaient de quatre ordres :

- la conformité de la directive 2006/24 à l'article 5, paragraphe 4, du TUE relatif à la proportionnalité des mesures législatives prises par l'UE,
- la compatibilité de la directive 2006/24 avec les articles 7, 8, 11 et 52 de la Charte des Droits Fondamentaux,
- les modalités d'interprétation et d'application de la Charte, notamment par rapport aux traditions constitutionnelles des États membres et au droit de la CEDH,
- l'interprétation de l'article 4, paragraphe 3, du TUE.

La Cour, comme l'Avocat Général, s'est focalisée sur les deux premières questions, tout en en circonscrivant le périmètre de façon plus précise.

Aucun élément particulier à souligner concernant le déroulement de la procédure, sinon qu'outre les parties aux litiges et les auteurs de la directive en cause, ont présenté des observations écrites et orales les gouvernements français, italien, polonais et britannique. C'est dire si l'enjeu était de taille, et ce tant pour les Etats membres que pour les sociétés et particuliers.

Pourtant, la décision rendue par la CJUE le 8 avril 2004 résonne comme un véritable paradoxe (**I**). Car les recours contre la directive 2006/24 et les mesures la transposant dans les droits nationaux se sont succédés, en vain, la Cour et la Commission ayant persisté pendant huit ans à considérer que cette disposition d'*harmonisation des législations* et non un dispositif de surveillance (**II**).

I. UN REVIREMENT ATTENDU, MAIS PARADOXAL

Une décision attendue. Alors même qu'elle était encore à l'état de discussion, la directive n° 2006/24 était l'objet d'une controverse. Sans surprise, les arguments des défenseurs des libertés fondamentales se mêlaient aux arguments technico-économiques des débiteurs de l'obligation de rétention de données. Les premiers voyaient dans ce *rapprochement des législations* la naissance d'un *Big Brother* numérique, tandis que les seconds évoquaient le poids économique induit par cette obligation. Près de dix ans plus tard, la Cour donnera raison aux premiers, tandis que les arguments des seconds auront été désamorcés par l'adoption par les Etats membres de mesures permettant une prise en charge – partielle – des frais.

Mais la directive interrogeait également les juristes des Etats membres. Le volume de données concernées par l'obligation de rétention – colossal – était considéré comme à l'origine d'atteintes à plusieurs droits fondamentaux : droit au respect de la vie privée, liberté d'expression, protection des individus à l'encontre des traitements de données. D'ailleurs, plusieurs cours constitutionnelles ont sanctionné les mesures de transposition de la directive critiquée : la Bulgarie, la Roumanie, l'Allemagne, Chypre, la Tchéquie. Et d'autres cours étaient en train de trancher lorsque sont intervenues les décisions commentées. En droit français, la question de la constitutionnalité aurait également pu se poser, le Conseil constitutionnel considérant un traitement de masse comme une atteinte au respect de la vie privée non proportionnée, qui plus est lorsqu'il peut être interrogé à d'autres fins que sa finalité principale (2).

Enfin, même la Commission s'attendait à cette issue. Car le jour même où la Cour rendait la décision commentée, Cecilia Malmström, commissaire européenne chargée des Affaires intérieures, faisait paraître un communiqué annonçant que cet arrêt « confirmait les conclusions critiques du rapport d'évaluation de 2011, notamment en ce qui concernait la proportionnalité des mesures » (3).

Mais une décision néanmoins surprenante. Bien qu'elle ait été attendue par tous, la décision commentée n'a pas manqué de surprendre. Une requête dans le moteur de recherche du site curia.europa.eu le met facilement en évidence : la directive n° 2006/24 a donné lieu à un abondant contentieux, donnant systématiquement raison aux autorités communautaires. Les recours en manquement initiés par la Commission ont été légion, la dernière requête, dirigée contre l'Allemagne, datant du 7 septembre 2012,

(1) Conclusions de l'avocat général, M. Pedro CRUZ VILLALÓN, présentées le 12 décembre 2013, §10.

(2) CC, 22 mars 2012, n° 2012-652-DC.

(3) http://europa.eu/rapid/press-release_STATEMENT-14-113_en.htm.

et les condamnations pécuniaires ont littéralement plu sur les Etats membres. Les Etats membres dont les Cour constitutionnelles avaient annulé les dispositions de transposition n'ont pas été épargnés, ce qui conduit au passage à s'interroger quant au respect par la Commission des « *traditions constitutionnelles communes aux États membres* », élément pourtant constitutif de « *l'ordre juridique de l'Union* » (4).

Mais la directive critiquée avait également donné lieu à un premier recours au fond, recours dans le cadre duquel la Cour avait rejeté la demande d'annulation présentée par l'Irlande, considérant que le Parlement européen et le Conseil de l'Union européenne s'étaient fondés, à juste titre, sur l'article 95 du Traité CE pour l'adopter (5). En clair, la Cour avait considéré que la directive relevait bel et bien du *1er pilier*, ses dispositions étant « *essentiellement limitées aux activités des fournisseurs de services et ne [réglementant] pas l'accès aux données ni l'exploitation de celles-ci par les autorités policières ou judiciaires des États membres* » (6). Et c'est essentiellement sur ce point que la solution ne manque pas d'étonner. Le considérant 21 de la directive précise certes que l'objectif poursuivi tend au rapprochement des législations, mais il poursuit en indiquant que l'objectif final était que les « *données soient disponibles aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne* ». Mieux, cinq ans plus tard, la Cour revenait sur ses conclusions, considérant que « *si la directive 2006/24 est destinée à harmoniser les dispositions des États membres relatives aux obligations desdits fournisseurs en matière de conservation de certaines données qui sont générées ou traitées par ces derniers, l'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1er, paragraphe 1, à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* » (7). La pirouette juridique n'échappera à personne.

II. LA PROHIBITION DE LA SURVEILLANCE DE MASSE

A. Une ingérence justifiée dans les droits fondamentaux

1. Les droits en cause

Les droits en cause. Les juridictions irlandaises et autrichiennes interrogeaient la Cour quant à la compatibilité de la directive critiquée avec les articles 7, 8 et 11 de la Charte des Droits Fondamentaux de l'UE. Mais la Cour ne retiendra que le droit au respect de la vie privée et le droit à la protection des données personnelles, considérant qu'il n'y avait plus lieu d'examiner une éventuelle atteinte à la liberté d'expression et d'information (8). Pourtant, l'Avocat Général avait considéré que « *les imprécisions de la demande préjudicielle de la High Court ainsi relevées ne sauraient toutefois conduire la Cour à rejeter celle-ci comme irrecevable* » (9). Certes, la Cour n'a pas déclaré irrecevable la saisine sur ce point. Mais dès lors qu'elle relevait que « *la conservation des données en cause [pouvait] avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication visés par cette directive et, en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte* » (10), on aurait aimé un arrêt plus prolixe sur ce point.

L'inférence et la liberté d'expression. Ceci est d'autant plus vrai que la Cour aborde au paragraphe 27 de l'arrêt une question qui devrait sous peu revêtir une importance particulière avec l'arrivée du *Big Data* : l'inférence. Les traitements de données ont ceci de particulier qu'ils permettent de produire des informations qui n'existaient pas a priori (11). Et tel est le cas des données de connexion, comme le relève à juste titre la Cour de Justice. Ainsi la géolocalisation des terminaux mobiles permet-elle par exemple d'inférer « *les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* ». De la même façon, la géolocalisation et l'horodatage peuvent permettre de déduire des informations sur les opinions de l'émetteur et du destinataire de la télécommunication si on les recoupe avec un agenda recensant des manifestations publiques, par exemple. L'impact de la directive 2006/24 sur la liberté d'expression aurait donc mérité d'être étudié.

Vie privée et données personnelles. Restaient donc les articles 7 et 8. Contrairement à la liberté d'expression, le lien entre ces dispositions et la directive est jugé direct et spécifique (12). Mais précisons-le immédiatement, un léger regret marque à cet égard

(4) Le respect par l'Union européenne, B. MATHIEU, Cahiers du Conseil constitutionnel n° 18 (Dossier : Constitution et Europe) - juillet 2005.

(5) CJUE, 10 février 2009, n° C-301/06, §93.

(6) §80.

(7) §41.

(8) §70.

(9) Conclusions de l'avocat général, M. Pedro CRUZ VILLALÓN, présentées le 12 décembre 2013, §23.

(10) 28.

(11) Le Ministère de la Santé français en faisait l'expérience, il y a peu encore : http://reflets.info/fic2014-ces-administrations-francaises-qui-livrent-ce-que-vous-avez-de-plus-intime-a-des-tiers-google-xiti/.

(12) §29.

l'arrêt de la Cour. Celle-ci s'épargne en effet la tâche de délimiter le périmètre précis de la vie privée et de la protection des données personnelles.

Certes, la Cour précise que la protection des données à caractère personnel contribue à faire respecter la vie privée (13). Mais elle omet de rappeler que la notion de données à caractère personnel est plus large que celle de vie privée (14), comme l'avait pourtant relevé le Tribunal de Première Instance de l'UE en 2007 (15). Il semble ainsi en résulter une sorte d'asservissement de la donnée à caractère personnel à la notion de vie privée, ce qui ne manquera pas de poser des difficultés pour la mise en œuvre de la directive *Opendata II*.

Mais l'imprécision de la Cour sur ce point s'avère avoir un effet nuisible bien plus actuel. Tel est par exemple le cas lorsque pour analyser l'ingérence dans le droit à la vie privée, les juges relèvent que l'accès aux données de connexion s'analyse comme une dérogation « *au régime de protection du droit au respect de la vie privée, instauré par les directives 95/46 et 2002/58, à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques* » (16). L'imbrication de la vie privée et de la protection des données nuit à la lisibilité de deux droits fondamentaux, pourtant clairement distincts. En effet, les dérogations à l'article 8 de la Charte sont admises de façon plus souple que pour la vie privée. Et quelques lignes plus tard, la Cour précisera que « *que la conservation des données et l'utilisation ultérieure de celles-ci (…) sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées (…) le sentiment que leur vie privée fait l'objet d'une surveillance constante* ». Là encore, le mélange des genres pose problème. Les juges se réfèrent à l'article 7 de la Charte, tout en utilisant une terminologie spécifique à la directive 95/46 qui relèverait donc plutôt de l'article 8. Mais la différence entre le champ d'application de chacune de ces dispositions ressort ici de façon particulièrement prégnante. En effet, en admettant que l'absence d'information puisse être considérée comme une atteinte à la privée, le fait que la personne concernée soit tenue dans l'ignorance d'un traitement ne constitue pas une atteinte à l'article 8 (17). La confusion que la Cour semble opérer entre vie privée et protection des données aboutit ainsi à un regrettable affaiblissement du raisonnement.

2. L'ingérence dans les droits à la vie privée et à la protection des données

Des ingérences qui « *vont de soi* ». S'agissant de l'article 7, la Cour note que la sensibilité des informations ne constituant pas une condition de l'ingérence, l'obligation de conservation « *constitue en soi une ingérence* » (18). A titre surabondant, elle précise que la possibilité pour les autorités d'accéder aux données constitue une atteinte supplémentaire au droit au respect de la vie privée. Cependant, sur ce point, la Cour se focalise sur l'absence de règles spécifiques encadrant cet accès, laissant ainsi la porte ouverte au législateur – communautaire ou des Etats membres – pour ouvrir les données des *opérateurs de télécommunication* aux forces de l'ordre.

L'atteinte à la protection des données va également de soi, puisque la directive « *prévoit un traitement des données à caractère personnel* » (19). L'argument est ici particulièrement faible. En effet, l'article 8 prévoit un droit à la protection des données, reprenant succinctement les conditions de licéité posées par la directive 95/46 du 24 octobre 1996. Mais il n'interdit en aucun cas la mise en œuvre d'un traitement de données, même sans le consentement des personnes concernées. Heureusement d'ailleurs, ce sans quoi l'informatisation de la justice et de la police serait sérieusement remise en cause. La Cour aurait donc pu faire l'effort de justifier ce en quoi la conservation des données constituait une atteinte à l'article 8. Ceci est d'autant plus désolant que la démonstration sera faite dans un second temps, lorsque la Cour examinera les conditions d'admissibilité d'un dispositif de rétention des données.

Des ingérences particulièrement graves. La Cour s'attache ensuite à examiner la gravité de l'atteinte à la vie privée et à la protection des données personnelles. Là encore, le raisonnement pourrait à première vue paraître léger, puisque cette gravité résulterait *simplement* de la « *vaste ampleur* » de l'ingérence. Mais il faut ici lire la décision entre les lignes : l'atteinte aux droits garantis par les articles 7 et 8 de la Charte est grave parce qu'il s'agit d'un *traitement de masse*. C'est l'extrême généralité du champ d'application de la directive qui menace la vie privée et le droit à la protection des données. Tous les moyens de communication « *grand public* » sont concernés, les données de connexion de tous les utilisateurs sont conservées.

Mais la Cour a considéré que l'argument ne suffisait pas. Elle a ainsi ajouté que la gravité de l'atteinte tenait également au *sentiment* de surveillance constante consécutif à l'absence d'information quant à l'enregistrement des données de connexion. Peut-être est-ce ici une erreur de traduction, même si le

(13) §48 et 53.

(14) Pour un exemple frappant sous l'empire de la loi n° 78-17 du 6 janvier 1978 dans sa version antérieure à la réforme de 2004 : CE, 30 mars 1990, Mme Degorge Boëtte, n° 90237.

(15) TPI, 8 novembre 2007, The Bavarian Lager Co.Ltd, T-194/04.

(16) §32.

(17) Cf. art. 7 de la directive 95/46 du 24 octobre 1995.

(18) §33.

(19) §36.

terme *feeling* est également utilisé dans la version anglaise de l'arrêt. Mais il semble regrettable qu'on puisse apprécier la gravité d'une ingérence dans le droit au respect de la vie privée en fonction de ce que peuvent ressentir des personnes qui ne sont pas victimes d'une atteinte, mais qui se pensent victimes.

3. Des ingérences justifiées

L'atteinte à un droit garanti par la Charte n'est illicite que si l'ingérence ne respecte pas le contenu essentiel desdits droits et n'est pas proportionnelle à l'objectif poursuivi, cette proportionnalité devant s'analyser au regard de la nécessité et de la pertinence des mesures litigieux pour réaliser les objectifs d'intérêt général poursuivis (20). La Cour s'est donc livrée à l'analyse de la justification de l'atteinte à la vie privée et à la protection des données.

Le contenu essentiel des droits est respecté. Les juges ont ainsi considéré que les dérogations posées par la directive critiquée ne vidaient pas les articles 7 et 8 de leur substance. En effet, le texte ne permet pas la prise de connaissance du contenu de la communication électronique, ces données n'étant pas conservées, et il met en place une « *règle relative à la protection et à la sécurité des données* » (21).

A ce stade du raisonnement, on ne peut que s'étonner. Car quelques paragraphes plus haut, la Cour avait esquissé un raisonnement sur l'inférence au terme duquel elle indiquait que les données de connexion étaient « *susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* ». Si la Cour avait examiné la directive à l'aune de l'article 11 de la Charte, peut-être l'aurait-elle donc annulée sur ce fondement, et non pas *simplement* en raison du caractère disproportionné de l'atteinte aux droits garantis aux articles 7 et 8 ? Mais de la sorte, n'aurait-elle pas sévèrement hypothéqué les chances pour le législateur communautaire d'adopter des mesures de remplacement ? Faut-il voir ici de la *politique jurisprudentielle* plus que du droit pur ?

La directive poursuit un objectif d'intérêt général. La pirouette juridique réalisée par la Cour pour revenir sur sa décision de 2009 et annuler la directive critiquée prend ici tout son sens. Si la directive n'avait eu pour objectif que d'harmoniser les législations, principal objectif retenu dans l'arrêt *Irlande c/ Commission*, cette condition n'aurait certainement pas été remplie. En développant la théorie de « *l'objectif matériel* », la Cour peut considérer que la lutte contre la criminalité constitue effectivement un objectif d'intérêt général. Quel intérêt ? Garantir l'efficience de la Charte, tout en laissant entrevoir au législateur communautaire une porte de sortie. Ne pas condamner la législation sur la rétention de données par principe. Là encore, on peut s'interroger quant à savoir s'il ne s'agit pas plus de *politique jurisprudentielle* que d'une volonté de la Cour de camoufler l'erreur commise dans sa décision de 2009.

B. Mais une ingérence disproportionnée

C'est donc au niveau de la proportionnalité que le bât blesse. Bien qu'elle n'exerce sur ce point qu'un *contrôle restreint* et qu'elle ait considéré que la conservation constituait une mesure pertinente pour assurer l'objectif *matériel* de la directive, la Cour a considéré que l'ampleur de la rétention n'était pas nécessaire. La Cour a critiqué de façon générale un manque de clarté et de précision dans la définition de la portée de l'obligation de conservation et des conditions d'accès aux données. Cette carence du législateur communautaire fait planer l'ombre d'accès illicites aux données sur le respect de la vie privée, et ce que l'illicéité résulte de l'identité de l'accédant, de la finalité qu'il poursuit ou du motif de l'accès.

Un arrêté pédagogique. Ceci étant, les derniers paragraphes de l'arrêt, détaillant le caractère disproportionné de l'ingérence dans les droits au respect de la vie privée et à la protection des données, peuvent se lire comme un *mode d'emploi* à l'usage de la Commission en prévision de l'élaboration d'une mesure de remplacement. En effet, pour chaque manquement constaté, la Cour prend soin d'indiquer jusqu'où le législateur peut aller.

1. L'enregistrement des données de connexion

Interdiction des traitements de masse. L'obligation de conservation des données vise tous les modes de communications électroniques accessibles au grand public sans cibler une catégorie de personnes particulières. La quasi-totalité de la population, excepté en fait les principaux acteurs de la criminalité organisée que l'on peut raisonnablement considérer comme utilisant les quelques moyens de communication insusceptibles d'être *enregistrés*, est donc concernée. La disproportion est manifeste. Les traitements de masse sont condamnés de façon quasi unanime par les Cours constitutionnelles des Etats membres.

La directive aurait ici dû se focaliser sur « *les personnes (…) se [trouvant], même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales* » (22). Mieux, le législateur communautaire aurait dû s'inspirer des dispositions du Code de Procédure Pénale français en matière de contrôle d'identité et

(20) Art. 52.

(21) §40.

(22) §58.

limiter la conservation aux données soit « *afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave* », soit relatives à « *des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves* » (23). La Cour exige en fait un dispositif de surveillance qui ne puisse être mis en œuvre qu'en présence d'un lien entre les données à conserver et une menace pour la sécurité publique.

Et les caractéristiques de cette menace devront également être définies – de manière objective – dans le texte de remplacement. La CJUE reproche en effet à la directive 2006/24 de renvoyer « *de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne* ».

Conciliation de la mesure avec le secret professionnel. La surveillance de masse mise en place par la directive critiquée pose une question plus grave encore que le simple respect de la vie privée : celle du respect du secret professionnel. La Cour n'aurait-elle pas tenté ici de faire comprendre à son principal lecteur le risque d'atteinte aux articles 48§2 de la Charte et 6§1 de la Convention Européenne des Droits l'Homme ? Une chose est certaine, quand bien même il s'agirait là d'une surinterprétation des intentions de la CJUE, le prochain texte devra concilier les impératifs de la lutte contre la grande criminalité et le terrorisme avec les droits de la défense.

2. L'accès aux données de connexion

Restriction d'accès. Le texte de remplacement de la directive 2006/24 devra également définir les conditions d'accès aux données. La directive annulée par la Cour ne fixait ni la liste des personnes pouvant accéder aux données, ni les conditions matérielles et procédurales de cet accès. Plus grave encore, le texte ne prévoyait pas expressément une restriction de l'accès et l'utilisation ultérieure des données à des fins de prévention et de détection d'infractions graves. La directive aurait donc pu être détournée de son fameux *objectif matériel*. Or, le respect de la vie privée impose que seuls les pouvoirs publics puissent accéder aux données de connexion, et ce uniquement dans des cas où une menace pour la sécurité publique existerait.

Contrôle d'accès. Mais la Cour va plus loin encore en exigeant que l'accès aux données soit réalisé sous le contrôle d'une juridiction ou d'une autorité indépendante (24). L'option ouverte ici par la Haute Juridiction tient ici à la dualité des droits en cause. En principe, une atteinte à la vie privée pour des motifs répressifs est placée sous le contrôle du juge, mais en matière de données personnelles, l'article 8§3 de la Charte précise « *le respect de ces règles est soumis au contrôle d'une autorité indépendante* », faisant ici clairement référence aux autorités de protection des données mises en place par la directive 95/46 du 24 octobre 1995. Le législateur communautaire aura ici probablement des difficultés à trancher entre l'une et l'autre de ces instances. L'idéal serait sans doute de coupler les deux, mais le dispositif pourrait alors perdre considérablement en flexibilité. Une solution résiderait sans doute ici à imposer que les mesures de transposition en droit national soient soumises au préalable à l'autorité de protection des données locales, tandis que le contrôle de l'accès aux données sera assuré par le juge.

3. La conservation des données

Une durée de connexion à définir et à adapter. La directive 2006/24 permettait aux Etats membres de conserver les données pendant une durée allant de six à vingt-quatre mois. Dans l'arrêt commenté, il est fait grief au législateur de ne pas avoir, une fois encore, donné des critères objectifs pour la détermination de cette durée. Le renvoi aux dispositions de la directive 96/46 est d'autant plus manifeste qu'à l'instar de la CNIL, la Cour recommande au législateur communautaire de prévoir une adaptation de la durée de conservation aux différentes catégories de données traitées.

Sécurité des données. Le Parlement et le Conseil vont enfin devoir se pencher sur la question de la sécurité des données de connexion conservées afin de proposer des garanties suffisantes. La directive 2006/24 ne prévoyait en effet aucune disposition spécifique, ne prenant pas en compte la sensibilité et la volumétrie de données, et elle n'imposait pas non plus aux Etats membres d'en adopter. La rigueur de la Cour mérite ici d'être soulignée. En effet, les juges auraient pu être tentés de considérer que la directive annulée ne dérogeait pas aux dispositions des directives 95/46 et 2002/58 quant à l'obligation de confidentialité des données, et ainsi admettre que le droit commun imposait déjà aux Etats membres de prendre des mesures de sécurité adéquates. Mais ils ont relevé la possibilité pour les fournisseurs de services de communication de prendre des mesures proportionnées aux « *considérations économiques* » relatives aux « *coûts de mise en oeuvre des mesures de sécurité* ». Le texte de remplacement qui sera certainement présenté au Parlement européen devra donc supprimer la possibilité pour les opérateurs d'adapter les mesures de sécurité en fonction de leur coût, et non pas de la sensibilité des données conservées. Nul doute que ce point donnera lieu à de nouveaux débats.

Sort des données à l'issue de la durée de conservation. Et la sévérité des juges quant à la sécurité des

(23) §59.

(24) §62.

données ne s'arrête pas là. Ils font ensuite grief à la directive 2006/24 de ne pas garantir « *la destruction irrémédiable des données au terme de la durée de conservation* ». Ici, c'est presque la rigueur des juges qui semble disproportionnée. Car il était-il vraiment nécessaire de rappeler dans la directive 2006/24 que la destruction des données au-delà de la période légale de conservation était obligatoire alors qu'une telle mesure est prévue résulte du droit commun, tel qu'il résulte tant de la directive 95/46 que de la directive 2002/58 ?

4. Lieu d'hébergement des données

Les raisons pour lesquelles la Cour a accordé une telle importance à la sécurité des données transparaissent clairement lorsqu'elle aborde la question du lieu d'hébergement des données.

Un hébergement en UE. Reprenant un sujet qui est cher au législateur français en matière de données de santé (25) et tenant manifestement compte des révélations d'Edward Snowden, la CJUE reproche à la directive 2006/24 de ne pas avoir imposé la conservation des données sur le territoire de l'Union. Ainsi que l'auront relevé tous les lecteurs de la directive 95/46, cette précision est purement dictée par le contexte, puisqu'en matière de protection des données, les transferts de données vers des Etats en dehors de l'UE sont admis dès lors qu'un niveau de protection adéquat des données est garanti. La Cour semble de la sorte conforter l'idée selon laquelle la sensibilité des données peut justifier une interdiction de les héberger ailleurs qu'en UE.

Mais le législateur communautaire devra-t-il aller plus loin ? Mais la Cour n'a pas « *déroulé le film* » jusqu'à son terme. Dans une décision du 31 juillet 2014 du *US District Court of New York*, la justice a posé le principe selon lequel tout prestataire américain de services de communication électronique est tenu de fournir les données échangées par le biais de ses services aux autorités américaines, quand bien même les données seraient hébergées en UE. Une question évidente se pose alors. Le législateur communautaire fera-t-il ici primer l'égalité de traitement des prestataires de service sur l'article 8 de la Charte ou considérera-t-il que la confidentialité des données personnelles justifie des restrictions vis-à-vis des prestataires américains ?

Vraisemblablement, tout dépendra ici d'une part des conclusions auxquelles aboutiront l'UE et les Etats-Unis quant à la confidentialité de ce qu'outre-Atlantique on appelle des « *oversea-data* », d'autre part des suites que les nouvelles instances européennes réserveront au projet de Règlement Général relatif à la Protection des Données. Mais quelle que soit la solution qui sera apportée aux pratiques américaines en terme de surveillance de masse, gageons que le texte qui viendra remplacer la directive 2006/24 ne pourra intervenir que postérieurement. ■

(25) Art. L1111-8 du Code de la Santé Publique.

L'arrêt de la Cour (grande chambre) du 8 avril 2014
est consultable à l'adresse suivante :
http://alineabyluxia.fr/eu/jp/2014/4/8/62012CJ0293