Recueil Dalloz 2014 p.1355

L'invalidation de la directive n° 2006/24/CE par la CJUE : une onde de choc en faveur de la protection des données personnelles

Céline Castets-Renard, Professeur de droit privé, Université Toulouse 1 Capitole, IRDEIC - Centre d'excellence Jean Monnet, Co-directrice du Master 2 Droit et informatique

La question de la protection des données personnelles est plus que jamais d'actualité en droit de l'Union européenne. Après le vote au mois de mars du « Paquet données personnelles »(1) par le Parlement européen dans sa composition précédente, la Cour de justice s'est à son tour posée en défenseur du droit fondamental à la vie privée et à la protection des données personnelles, consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne(2). La décision rendue le 8 avril 2014 par la Cour de justice de l'Union européenne (CJUE) dans deux affaires jointes(3) invalide la directive n° 2006/24/CE 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. Si la Cour de justice estime que la conservation des données des communications électroniques est utile dans la lutte contre certaines infractions comme le terrorisme, elle juge qu'elle n'en constitue pas moins une ingérence dans la vie privée des individus qui, bien que justifiée, s'avère disproportionnée.

Dans la première affaire (aff. C-293/12), l'organisation irlandaise *Digital Rights* de défense des droits fondamentaux sur l'internet a introduit le 11 août 2006 un recours devant la *High Court*. Propriétaire d'un téléphone portable ayant été enregistré, elle met en cause la légalité de mesures législatives et administratives nationales(4) concernant la conservation de données relatives à des communications électroniques transposant la directive n° 2006/24/CE. La *High Court* a considéré qu'il fallait examiner la validité de la directive n° 2006/24/CE, ayant modifié la directive n° 2002/58/CE (Dir. « Vie privée et communications électroniques »), et a saisi la Cour de justice pour lui soumettre trois questions préjudicielles. La Cour de justice n'examine que la première relative à la compatibilité de ladite directive avec le droit au respect de la vie privée (art. 7 de la Charte et art. 8 de la Conv. EDH), ainsi qu'avec le droit à la protection des données à caractère personnel (art. 8 de la Charte) et le droit à la liberté d'expression (art. 11 de la Charte et art. 10 de la Conv. EDH). La même question a été posée dans la deuxième affaire (aff. C-594/12) par le *Verfassungsgerichtshof* (juge autrichien).

Dans son contrôle du respect du droit secondaire au droit primaire, la Cour de justice pointe l'incompatibilité de ces normes. Elle invalide la directive n° 2006/24/CE dont l'ingérence dans les droits fondamentaux est, certes, justifiée (I) mais disproportionnée, d'autant que la sécurité dans la protection des données personnelles n'est pas garantie (II). Cette décision radicale ne surprend pas car la directive n° 2006/24/CE est critiquée depuis plusieurs années.

I - L'ingérence justifiée de la directive n° 2006/24/CE dans les droits fondamentaux

La Cour de justice n'a aucune difficulté à établir que l'obligation de conservation de données de communication prévue par la directive n° 2006/24/CE constitue une ingérence dans les droits fondamentaux des individus (A) qui trouve toutefois une justification dans la lutte contre la criminalité (B).

A - L'ingérence dans la protection de la vie privée et des données personnelles

Aux fins de les rendre accessibles aux autorités nationales compétentes, les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications ont l'obligation de conserver les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile (art. 3 et 5). Figurent ainsi le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services internet. Ces données permettent de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une certaine période. De telles données renseignent sur les habitudes de vie quotidienne des personnes, leurs lieux de séjour permanents ou temporaires, leurs déplacements réguliers, leurs activités, leurs relations sociales et milieux sociaux. Dès lors, même si la directive n° 2006/24/CE interdit la conservation du contenu de la communication et des informations consultées en utilisant un réseau de communications électroniques (art. 1er, § 2, et art. 5, § 2), la conservation des données susvisées peut avoir une incidence sur la liberté d'expression des abonnés (art. 11 de la Charte), la protection de la vie privée et des communications (art. 7 de la Charte), la protection des données à caractère personnel (art. 8 de la Charte)(5). La conservation des données dans le secteur des communications électroniques constitue une dérogation au régime de protection des directives n° 95/46/CE et n° 2002/58/CE qui posent le principe de confidentialité des communications et données relatives au trafic, ainsi que l'obligation de les effacer ou de les rendre anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication.

L'obligation de conservation imposée par la directive n° 2006/24/CE constitue à l'évidence une ingérence dans les droits fondamentaux, peu important que les informations conservées aient un caractère sensible ou que les intéressés aient subi d'éventuels inconvénients(6). En outre, l'accès des autorités nationales compétentes aux données entraîne une ingérence supplémentaire(7) et l'ingérence ainsi organisée par ladite directive est d'une vaste ampleur. Elle doit donc être considérée comme particulièrement grave, d'autant que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés, ce qui peut laisser croire à une surveillance constante de leur vie privée.

B - La justification de l'ingérence dans la lutte contre la criminalité

Si l'ingérence ne fait aucun doute, elle peut toutefois trouver une justification à l'article 52, § 1, de la Charte qui prévoit des limitations dans l'exercice des droits et libertés consacrés. Autrement dit, les droits reconnus sont fondamentaux, sans pour autant être absolus. Les limitations doivent toutefois être prévues par la loi, respecter leur contenu essentiel, ainsi que le principe de proportionnalité, être nécessaires et répondre effectivement à des

objectifs d'intérêt général reconnus par l'Union ou de protection des droits et libertés d'autrui.

S'agissant du contenu essentiel des droits fondamentaux, l'ingérence n'est pas de nature à porter atteinte, puisque la directive n° 2006/24/CE interdit de prendre connaissance du contenu des communications électroniques. En outre, son article 7 prévoit l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données. Ensuite, l'ingérence répond à un objectif d'intérêt général, car la directive n° 2006/24/CE vise à garantir la disponibilité des données conservées à des fins de recherche, de détection et de poursuite d'infractions graves. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave. Selon la jurisprudence de la Cour, constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international(8), ainsi que la lutte contre la criminalité grave, afin de garantir la sécurité publique(9). Par ailleurs, l'article 6 de la Charte énonce le droit de toute personne à la liberté, mais également à la sûreté. En outre, le Conseil « Justice et affaires intérieures » du 19 décembre 2002 a relevé que les données relatives à l'utilisation de communications sont utiles à la prévention des infractions et la lutte contre la criminalité. La conservation des données répond bien à un objectif d'intérêt général.

L'usage des technologies de l'information et de la communication (TIC) facilite la commission d'infractions, aussi est-il nécessaire de permettre aux autorités de police de contrôler les individus par ces procédés. En particulier, le téléphone mobile et internet constituent aujourd'hui des moyens de communication essentiels par lesquels une surveillance efficace peut être mise en oeuvre. En outre, les TIC sont de très bons outils de surveillance en tant que tels et permettent tout particulièrement de satisfaire l'objectif de sécurité. L'adoption récente en France de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire (art. 20) et de la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation(10) témoigne de cette tentation d'une surveillance accrue des individus, ce qui n'est pas sans créer de tensions dans la protection des droits fondamentaux. En l'espèce, la directive n° 2006/24/CE répond à cet objectif de sécurité nationale mais doit encore satisfaire le principe de proportionnalité.

II - L'ingérence disproportionnée de la directive n° 2006/24/CE dans les droits fondamentaux

L'ingérence est justifiée mais s'avère disproportionnée (A), d'autant que la sécurité des données n'est pas garantie (B).

A - Le contrôle strict de proportionnalité de l'ingérence

Selon une jurisprudence constante de la Cour(11), le principe de proportionnalité exige que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs. Le respect de ces conditions fait l'objet d'un contrôle juridictionnel et, dès lors que des ingérences dans des droits fondamentaux sont en cause, le pouvoir d'appréciation du législateur de l'Union peut s'avérer limité, en fonction, notamment, du domaine concerné, de la nature du droit en cause garanti par la Charte, de la nature et la gravité de l'ingérence ainsi que de la finalité de celle-ci(12). En l'espèce, compte tenu du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et de l'ampleur et de la gravité de l'ingérence dans ce droit résultant de la directive n° 2006/24/CE, le pouvoir d'appréciation du législateur de l'Union doit être réduit.

Le juge exerce donc un contrôle strict. Il doit vérifier si la conservation des données permet de réaliser l'objectif poursuivi par la directive n° 2006/24/CE. Eu égard à l'importance croissante des moyens de communications électroniques, les données conservées permettent aux autorités nationales compétentes de disposer de moyens utiles pour élucider des infractions graves. L'efficacité de la lutte contre la criminalité grave peut dépendre amplement de l'utilisation des techniques modernes d'enquête. L'objectif poursuivi est alors atteint, peu important qu'il existe par ailleurs d'autres modalités de communications électroniques ou autorisant une communication anonyme.

Toutefois, bien que fondamental, un tel objectif d'intérêt général ne saurait à lui seul justifier qu'une mesure de conservation soit considérée en soi comme nécessaire aux fins de ladite lutte. Il convient, par ailleurs, de considérer le droit fondamental au respect de la vie privée(13) et à la protection des données à caractère personnel, dont les limitations doivent être strictement nécessaires(14), *a fortiori* si les données sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données(15). Or la Cour relève que la directive n° 2006/24/CE couvre de manière généralisée tous les abonnés et utilisateurs inscrits, tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun, ainsi que l'ensemble des données relatives au trafic, sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre les infractions graves. Notamment, il n'est pas exigé que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Ladite directive n'est pas non plus limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées à une infraction grave. Au demeurant, la directive n° 2006/24/CE ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure. Elle se borne à renvoyer de manière générale aux infractions graves, telles que définies par chaque Etat membre. De même, aucune condition matérielle ni procédurale d'accès aux données n'est prévue et chaque Etat membre arrête la procédure à suivre dans le respect des exigences de nécessité et de proportionnalité, sans qu'aucun critère objectif n'ait été posé ou attendu des Etats, ni contrôle préalable, soit par une juridiction, soit par une entité administrative indépendante. Enfin, la directive n° 2006/24/CE impose la conservation des données pendant une période entre six mois et vingt-quatre mois, sans distinction entre catégories de données, personnes concernées ou d'autres critères objectifs, afin d'être limitée au strict nécessaire.

Cette argumentation n'est pas sans rappeler la position du Parlement européen lors de l'adoption du « Paquet données personnelles » le 12 mars 2014, plus précisément de la Résolution sur le programme de surveillance de la NSA(16). Les eurodéputés ont estimé que les mesures de sécurité, notamment dans le cadre de la lutte contre le terrorisme, doivent respecter les obligations en matière de droits de l'homme. Si les gouvernements affirment que les programmes de surveillance de masse sont nécessaires à la lutte contre le terrorisme et dénoncent fermement le terrorisme, cette lutte ne peut en aucun cas justifier l'existence de programmes de surveillance de masse non ciblés, secrets, voire illégaux. En fin de compte, ces programmes ont été considérés incompatibles avec les principes de nécessité et de proportionnalité en vigueur dans les sociétés démocratiques.

En l'espèce, la directive n° 2006/24/CE ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est ainsi de constater que l'ingérence est d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union. La Cour invalide donc la directive. Cette décision n'étonne pas car la Commission européenne avait lancé dès 2009 un processus

d'évaluation de la directive qui a donné lieu à un rapport en 2011 (17). Elle en concluait à une transposition inégale de la directive, à une harmonisation insuffisante et admettait également que la proportionnalité dans le processus de stockage et conservation des données n'était pas garantie, dans la lignée de l'avis du Contrôleur européen pour la protection des données personnelles (CEPD) rendu le 31 mai 2011 (18). Ce dernier avait exprimé de sérieux doutes sur la nécessité et la proportionnalité des mesures et dénoncé aussi une trop grande marge de manoeuvre des Etats membres concernant les finalités d'utilisation des données et les conditions d'accès. Une révision de la directive avait été envisagée mais n'avait pas vu le jour. La Cour contraint désormais la Commission européenne à reformuler un texte plus équilibré.

B - La sécurité insuffisante de la protection des données personnelles

Outre le caractère disproportionné de l'ingérence, la Cour de justice relève l'absence de garanties et règles précises dans la sécurité et la protection des données personnelles conservées par les fournisseurs de services de communications électroniques. En particulier, la directive n° 2006/24/CE ne prévoit aucune protection efficace pour garantir la pleine intégrité et confidentialité contre les risques d'abus, ainsi que contre tout accès et toute utilisation illicites de ces données. Aucune mesure technique ou organisationnelle n'est prônée. En outre, les opérateurs sont autorisés à tenir compte des coûts de mise en oeuvre des mesures de sécurité et sont donc amenés à faire des arbitrages. Il est évident qu'ils ne peuvent appliquer un niveau élevé de protection pour toutes les données, compte tenu du coût exorbitant que cela représenterait. Enfin, la directive n° 2006/24/CE ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci. Il s'agit là de l'un des points faibles majeurs de la législation sur les données personnelles que l'on retrouve aussi dans l'application de la directive n° 95/46/CE. Le respect du principe de finalité est difficile à garantir et il faut souhaiter que la réforme prévue par la proposition de règlement du 25 janvier 2012 permette de mieux satisfaire cette exigence grâce au renforcement des sanctions.

La Cour de justice ajoute, par ailleurs, que la directive n° 2006/24/CE n'impose pas que les données en cause soient conservées sur le territoire de l'Union, de sorte que n'est pas pleinement garanti le contrôle, pourtant essentiel (19), du respect des exigences de protection et de sécurité par une autorité indépendante (art. 8, § 3, de la Charte). Le contrôle du respect de la législation sur les données personnelles est confié aux autorités indépendantes nationales comme la Commission nationale de l'informatique et des libertés (CNIL), ainsi qu'au CEPD concernant l'Union. La proposition de règlement du 25 janvier 2012 confirme cette logique en renforçant les pouvoirs de ces autorités, ainsi que les exigences relatives à leur indépendance. Au-delà, la question soulevée ici par la Cour de justice est celle du lieu de conservation des données, à l'heure du *cloud computing* proposé par des opérateurs stockant souvent les données en dehors de l'Union. Un *cloud computing* souverain européen est appelé de ses voeux par le Parlement européen (Résolution du 12 mars 2014) pour pallier cette difficulté.

A la suite de l'invalidation de la directive n° 2006/24/CE par la Cour de justice en raison de la violation du principe de proportionnalité au regard des articles 7, 8 et 52, § 1, de la Charte, la Commission et le nouveau Parlement européen vont devoir enfin procéder à la réécriture de la directive, pourtant envisagée par la Commission dès 2011. En définitive, si la décision de la Cour de justice pointe des difficultés déjà connues, elle a le mérite de l'efficacité et de faire cesser une situation peu respectueuse des droits fondamentaux des citoyens européens. Le texte qui prendra le relais devra mieux les protéger, ce qui devrait se traduire par une réduction de la marge de manoeuvre des Etats et par des conditions plus strictes dans la conservation des données liées aux communications électroniques. Le juge pousse ici le législateur à réagir et ce n'est pas le moindre mérite de l'arrêt du 8 avril 2014.

Mots clés :
UNION EUROPEENNE * Internet * Communication électronique * Données * Conservation * Modalités

(1) Proposition de règlement du Parlement et du Conseil 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 du 25 janv. 2012 (COM(2012) 0011) et proposition de directive à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (COM(2012) 0010).

(2) V. aussi : CJUE 13 mai 2014, aff. C-131/12, *Google Spain c/ Agencia Española de Protección de Datos*, D. 2014. 1092 , et les notes de V.-L. Benabou, N. Martial-Braz et J. Rochfeld, *à paraître*.

(3) D. 2014. 871 ; AJDA 2014. 773 .

(4) *Criminal Justice (Terrorist Offences) Act* (2005).

(5) CJUE 9 nov. 2010, aff. C-92/09 et C-93/09, *Volker und Markus Schecke* et *Eifert*, pt 47 ; RTD eur. 2011. 375, chron. A. Potteau .

(6) CJUE 20 mai 2003, aff. C-465/00, C-138/01 et C-139/01, *Österreichischer Rundfunk e.a.*, pt 75 ; AJDA 2003. 2146, chron. J.-M. Belorgey, S. Gervasoni et C. Lambert .

(7) Concernant l'art. 8 de la Conv. EDH : arrêts CEDH 26 mars 1987, n° 9248/81, *Leander c/ Suède*, série A, n° 116, § 48 ; 4 mai 2000, n° 28341/95, *Rotaru c/ Roumanie [GC]*, § 46, Rec. CEDH 2000-V ; D. 2001. 1988 , obs. A. Lepage ; AJDA 2000. 1006, chron. J.-F. Flauss ; ainsi que 29 juin 2006, n° 54934/00, *Weber et Saravia c/ Allemagne* (déc.), § 79, Rec. CEDH 2006-XI.

(8) CJUE 3 sept. 2008, aff. C-402/05 P et C-415/05 P, *Kadi et Al Barakaat International Foundation c/ Conseil et Commission*, pt 363 ; D. 2009. 1118 , note D. Delcourt ; RFDA 2008. 1204, note P. Cassia et F. Donnat ; RSC 2009. 75, étude H. Rouidi , et 197, obs. L. Idot ; RTD eur. 2009. 161, note J. P. Jacqué ; 15 nov. 2008, aff. C-539/10 P et C-550/10 P, *Al-Aqsa c/ Conseil*, pt 130.

(9) CJUE 23 nov. 2010, aff. C-145/09, *Tsakouridis*, pts 46 et 47 ; AJDA 2010. 2240, et 2011. 264, chron. M. Aubert, E. Broussy et F. Donnat ; RTD eur. 2011. 604, obs. S. Robin-Olivier ; RMCUE 2013. 45, chron. E. Sabatakakis.

(10) JO 29 mars 2014, p. 6123 ; D. 2014. 780.

(11) CJUE 8 juill. 2010, aff. C-343/09, *Afton Chemical*, pt 45 ; D. 2010. 2468, obs. F. G. Trébulle ; 9 nov. 2010, aff. C-92/09, *Volker und Markus Schecke et Eifert*, pt 74 ; RTD eur. 2011. 375, chron. A. Potteau ; 23 oct. 2012, aff. C-581/10 et C-629/10, *Nelson e.a.*, pt 71 ; RTD eur. 2013. 372, obs. L. Grard ; 22 janv. 2013, aff. C-283/11, *Sky Österreich*, pt 50 ; D. 2014. 396, obs. N. Alaphilippe ; ainsi que 17 oct. 2013, aff. C-101/12, *Schaible*, pt 29.

(12) Par analogie avec l'art. 8 de la Conv. EDH : CEDH 4 déc. 2008, n° 30562/04 et n° 30566/04, *S et Marper c/ Royaume-Uni [GC]*, § 102, Rec. CEDH 2008-V ; D. 2010. 604, obs. H. Gaumont-Prat ; AJDA 2009. 872, chron. J.-F. Flauss ; AJ pénal 2009. 81, obs. G. Roussel ; RFDA 2009. 741, étude S. Peyrou-Pistouley ; RSC 2009. 182, obs. J.-P. Marguénaud.

(13) Par analogie avec l'art. 8 de la Conv. EDH : CEDH 1er juill. 2008, n° 58243/00, *Liberty et autres c/ Royaume-Uni*, § 62 et 63 ; *Rotaru c/ Roumanie*, préc., § 57 à 59 ; *S et Marper c/ Royaume-Uni*, préc., § 99.

(14) CJUE 7 nov. 2013, aff. C-473/12, *IPI*, pt 39.

(15) *Ibid*.

(16) N° 2013/2188(INI).

(17) Rapport d'évaluation de la Commission au Conseil et au Parlement européen du 18 avr. 2011 concernant la directive sur la conservation des données (Dir. n° 2006/24/CE) (COM(2011) 225 final).

(18) https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf.

(19) CJUE 16 oct. 2012, aff. C-614/10, *Commission c/ Autriche*, pt 37 ; RTD eur. 2013. 671, obs. F. Benoît-Rohmer.