Droit de l'Union et protection des données à caractère personnel

Marjolaine Roccati

Droit de l'Union et protection des données à caractère personnel

Alors que le Conseil rassemblant les ministreseuropéens de la Justice se penche actuellement sur uneréforme de la législation européennerelative à la protection des données à caractère personnel[1], il est utile de revenir sur le cadre juridique existant,en la matière, au sein de l'Union.

La pièce maîtresse : la directive 95/46/CE. Le texte de référence au sein de l'Union européenne est la directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2].

Le législateur européen avait alors justifié son interventionen invoquant l'article 100 A du Traité CE[3] relatif au rapprochement des législations des États membres pour les besoins de l'établissement et du fonctionnement du marché intérieur. Les progrès des technologies de l'information facilitant déjà le traitement et l'échange des données entre tous les acteurs privés ou publics de la vie économique et sociale des États membres[4], le marché intérieur nécessitait alors « non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés »[5]. La législation européenne en matière de protection des données personnelles s'est ainsi construite autour de ces deux objectifs : garantir la libre circulation des données et protéger le droit fondamental à la protection des données.

Objet de la directive 95/46/CE. L'objet de la directive 95/46 est d'imposer aux États membres l'obligation de garantir le droit à la vie privée des personnes physiques à l'égard du traitement de leurs données à caractère personnel[6], en vue de permettre la libre circulation de

[1] Voir Conseil JAI (« Justice et Affaires Intérieures »), 6 juin 2014 : « Les ministres enregistrent des progrès dans la réforme de la protection des données […] », accessible au lien suivant : http://www.europaforum.public.lu/fr/actualites/2014/06/conseil-jai-justice/index.html [consulté le 23 juin 2014].
[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.* n° L 281 du 23/11/1995, pp. 31-50.
[3] Moins strict que l'article 100, il a été introduit par l'Acte unique européen de 1986 – *J.O.*, L. 169 du 29 juin 1987, pp. 1-29– pour relancer le processus de rapprochement des législations ; il est devenu depuis l'article 95 TCE puis 114 TFUE.
[4]Directive 95/46/CE, 5ème considérant.
[5]*Ibid.*, 3ème considérant.
[6]*Ibid.*,article 1er § 1.

ces données entre les États membres[7]. La directive contient une série de règles définissant les conditions de licéité des traitements de données à caractère personnel[8]. Elle précise par ailleurs les droits des personnes dont les données sont collectées et traitées, en particulier le droit à l'information[9], le droit d'accès[10], le droit d'opposition[11] et le droit de recours[12]. Elle garantit par ailleurs la confidentialité et la sécurité des traitements[13].

L'article 29 de la directive a permis l'instauration d'un groupe de travail, composé notamment d'un représentant de l'autorité de contrôle désignée par chaque État membre – la CNIL en France. Ce groupe, au caractère consultatif et indépendant, a pour mission de contribuer à la mise en œuvre homogène des dispositions nationales prises en application de la directive et de conseiller la Commission européenne sur tout projet ayant une incidence sur le traitement des données à caractère personnel[14].À cette fin, le Groupe de travail ou G.T. « Article 29 » émet un certain nombre de recommandations[15].

Une interprétation extensive par la CJUE. La Cour de justice a adopté une interprétation extensive de la directive 95/46/CE pour l'adapter aux évolutions technologiques ultérieures, notamment au développement d'Internet.

C'est ainsi que dans un arrêt récent, sans suivre les conclusions plus prudentes de son avocat général[16], elle a appliqué la directive à un exploitant de moteur de recherche – en

[7]*Ibid.*, article 1er § 2.
[8]*Ibid.*,notamment article 6 : « 1. Les États membres prévoient que les données à caractère personnel doivent être:
a) traitées loyalement et licitement;
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées;
c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;
d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;
e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.
2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1 ».
[9]*Ibid.*,articles 10 et 11.
[10]*Ibid.*,article 12.
[11]*Ibid.*,article 14.
[12]*Ibid.*,article 22.
[13]*Ibid.*,section VIII.
[14]*Ibid.*,article 30.
[15] Voir par exemple Document de travail n°02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies, 2 octobre 2013, *1676/13/FR WP 208*.
[16]Conclusions de l'avocat général M. NiiloJääskinen présentées le 25 juin 2013 dans l'affaire *Google Spain*, aff. C-131/12.

l'espèce Google – institué « responsable du traitement » des données à caractère personnel qu'il trouve, indexe, stocke et met à disposition des internautes[17]. Par ailleurs, même si cette activité ne s'opère pas directement dans l'État membre concerné – ici l'Espagne –la Cour a considéré comme suffisant, aux fins du traitement, qu'une succursale ou filiale y assure la promotion et la vente des espaces publicitaires proposées par ce moteur de recherche et dont l'activité vise les habitants de cet État membre[18]. Une fois justifiée l'applicabilité de la directive 95/46/CE, la Cour en a déduit l'obligation pour l'exploitant du moteur de recherche de supprimer de la liste des résultats les informations qui apparaissent inadéquates, pas ou plus pertinentes ou excessives au regard des finalités du traitement en cause réalisé[19], alors même que leur publication en elle-même sur le web est licite[20].

L'intervention du législateur européen, quant à elle, est restée ponctuelle postérieurement à la directive de 1995.

Des instruments complémentaires concernant les communications électroniques. Le régime de protection des données personnelles établi par la directive 95/46/CEa été précisé et complété par des règles spécifiques applicables au secteur des communications électroniques[21]. Une première directive a été édictée le 15 décembre 1997, par la suite abrogée et remplacée par la directive 2002/58/CE du 12 juillet 2002[22]. Cette dernière comporte des règles imposant aux États membres de garantir la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public[23].

[17] C.J.U.E., 13 mai 2014, *Google Spain SL, Google Inc. c/ AgenciaEspañola de Protección de Datos (AEPD), Mario Costeja González*, aff. C-131/12, point 41.
[18] *Ibid.*, point 60.
[19] *Ibid.*, point 94.
[20] *Ibid.*, point 88.
[21] Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, *J.O.* n° L 24 du 30/01/1998, pp. 1-8.
[22] 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), *J.O.* n° L 201 du 31/07/2002, pp. 37-47.
[23] Article 5 § 1 de la directive 2002/58/CE ; voir ainsi article 6 : « Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication ».

De la libre circulation à uneobligation de conservationdes données ? La directive de 2002 a été suivie d'une directive du 15 mars 2006[24], qui prévoyait pour les États membres une obligation de collecte et de conservation des données de trafic et de localisation en vue de la prévention, recherche, détection et poursuite d'infractions pénales.

Cette directive a opéré une « modification profonde de l'état du droit applicable aux données afférentes aux communications électroniques »[25].En effet, dès 1995, les institutions européennes avaientdonné auxÉtats membres la possibilité de prendre des mesures législatives visant à limiter la portée d'obligations et de droits prévus à la directive lorsqu'une telle limitation était nécessaire pour sauvegarder un certain nombre d'objectifs listés, y compris la prévention, recherche, détection et poursuite d'infractions pénales[26]. La directive de 2002 y renvoyait expressément à son tour[27]. Toutefois, cette possibilité ouverte aux États membres était devenue source de disparités législatives sur la conservation des données, constitutive d'« entraves au marché intérieur des communications électroniques dans la mesure où les fournisseurs de services doivent satisfaire à des exigences différentes pour ce qui est des types de données relatives au trafic et à la localisation à conserver ainsi que des conditions et des durées de conservation »[28]. Le législateur européen a ainsijustifié l'édiction d'une obligation générale de conservation des données à travers la directive de 2006.

---

[24] 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, *J.O.* L 105 du 13 avril 2006, pp. 54-63.

[25] Conclusions de l'avocat général M. Pedro Cruz Villalon présentées le 12 décembre 2013 dans l'affaire *Digital Rights Ireland*, C-293/12 et C-594/12, point 36.

[26]Directive 95/46/CE, article 13 : « 1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:
a) la sûreté de l'État;
b) la défense;
c) la sécurité publique;
d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;
e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);
g) la protection de la personne concernée ou des droits et libertés d'autrui.
2. Sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, les États membres peuvent, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, limiter par une mesure législative les droits prévus à l'article 12 lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques. »

[27]Directive 2002/58/CE, article 15 § 1.

[28] Voir considérant 6 de la directive 2002/58/CE.

Le frein de la Cour de justice, gardienne des droits fondamentaux. L'obligation générale de conservation des données se caractérisait par sa généralité et l'absence d'encadrement de l'action des autorités nationales compétentes en la matière, à l'instar d'une possibilité de conservation des données pendant une période de six mois au minimum et vingt-quatre mois au maximum sans critère objectif de délimitation. En conséquence, la Cour de justice, incitée en ce sens par son avocat général[29], a constaté que l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel n'était pas encadrée par des dispositions permettant de garantir qu'elle était effectivement limitée au strict nécessaire. À l'issue d'un contrôle de proportionnalité révélant l'absence de règles claires et précises dans la directive assurant que les personnes dont les données étaient conservées disposaient de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites, la Cour a invalidé la directive de 2006[30], sans limiter dans le temps les effets de sa décision. Les dispositions nationales transposant la directive devraient ainsi être relues à la lumière de l'interprétation donnée par la Cour de justice, permettant peut-être par ce contrôle d'atteindre l'harmonisation à laquelle n'a pu parvenir le législateur de l'Union.

La décision-cadre 2008/977/JAI en matière pénale. À la directive de 1995 est venue s'ajouterune décision-cadre de novembre 2008 destinée, à titre d'instrument général au niveau de l'Union, à protéger les données à caractère personnel dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale[31]. En effet, un instrument distinct était nécessaire car la directive 95/46/CE ne pouvait pas s'appliquer dans le cadre d'une activité qui n'entrait pas dans le champ d'application du droit communautaire. En l'occurrence, la coopération policière et judiciaire en matière pénale ressortait du titre VI du traité sur l'Union européenne, troisième pilier reposant sur une structure intergouvernementale au sein de laquelle les compétences de la Commission européenne, du Parlement européen et de la Cour de justice des Communautés européennes étaient limitées au

[29]Conclusions de l'avocat général M. Pedro Cruz Villalon présentées le 12 décembre 2013.

[30] CJUE, 8 avril 2014, *Digital Rights Ireland Ltd (C-293/12) c/ Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlande, The Attorney General, en présence de: Irish Human Rights Commission, et KärntnerLandesregierung (C-594/12), Michael Seitlinger, ChristofTschohle.a.*, aff. jointesC‑293/12 et C‑594/12, spec. points 54 et suiv.

[31] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.* L 350 du 30.12.2008, pp. 60-71.

profit du Conseil de l'Union européenne et des États membres. La coopération policière et judiciaire en matière pénale a été intégrée au titre V du TFUE, aux articles 82 à 89, même si l'action des institutions européennes demeure encadrée.

Le cadre juridique de l'Union de la protection des données à caractère personnels'est affranchi par la suite du marché intérieur et de la coopération en matière pénale, pour s'inscrire dans tous les espaces de l'Union.

La protection des données à caractère personnel, inscrite à l'article 16 TFUE. Avec l'entrée en vigueur du traité de Lisbonne, l'article 16 TFUE énonce le droit de toute personne à la protection des données à caractère personnel la concernant. L'article donne ensuite compétence aux institutions européennes pour fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union[32].

Cet article est issu de l'article 286 du traité CE, introduit par le traité d'Amsterdam et entré en vigueur le 1er janvier 1999, qui prévoyait l'application aux institutions et organes de l'Union des actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[33]. Sur cette base, le règlement 45/2001[34] avait été adopté, qui institue notamment une autorité de contrôle indépendante, le Contrôleur européen, chargée de surveiller le traitement des données à caractère personnel par les institutions et organes de l'Union.

Au-delà de l'obligation pesant sur les institutions européennes, le traité institue désormaisun droit devant être respecté dans toute réglementation européenne. Ainsi, se fondant sur l'article 16 TFUE, la Commission européenne a proposé en janvier 2012 une

[32] Article 16 TFUE : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.
Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne ».

[33] Article 286 TCE : « 1. À partir du 1er janvier 1999, les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes institués par le présent traité ou sur la base de celui-ci.
2. Avant la date visée au paragraphe 1, le Conseil, statuant conformément à la procédure visée à l'article 251, institue un organe indépendant de contrôle chargé de surveiller l'application desdits actes communautaires aux institutions et organes communautaires, et adopte, le cas échéant, toute autre disposition utile. »

[34] Règlement (CE) n°45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.* L 8 du 12.01.2001, pp. 1-22.

réforme globale en matière de protection des données, à travers deux textes : un règlement général sur la protection des données à caractère personnel[35] et une directive sur le traitement et la circulation de données 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[36]. Ces deux textes sont actuellement en cours de discussion[37].

Parallèlement, la Charte des droits fondamentaux a consacré la protection des données à caractère personnel en tant que droit fondamental.

La protection des données à caractère personnel, droit fondamental garanti par la Charte. La Charte des droits fondamentaux, qui s'est vue confier en décembre 2009 la même force juridique obligatoire que les traités, consacre un article 8 à la « protection des données à caractère personnel ». Cet article prévoit notamment le traitement loyal de ces données, le droit d'accès et de rectification[38], soumis au contrôle d'une autorité indépendante[39]. Cet article complète l'article précédent qui garantit le « respect de la vie privée et familiale » (article 7). Les dispositions de la charte s'adressent aux institutions de l'Union et aux États membres lorsqu'ils mettent en œuvre le droit de l'Union[40]. Si la charte n'empêche pas toute limitation,sous réserve de poursuivre un objectif d'intérêt général et d'être limitée au strict nécessaire[41], elle conduit à rendre le droit à la protection de ses données à caractère personnel plus accessible pour tout justiciable de l'Union[42].

Marjolaine Roccati

23/06/2014

[35] Proposition de règlement du Parlement européen 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 (règlement général sur la protection des données), présentée le 25 janvier 2012 – COM(2012) 11 final.

[36] Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, présentée le 25 janvier 2012 – COM(2012) 10 final.

[37] Voir le site « PreLex » sur Europa.eu

[38] Charte des droits fondamentaux, article 8 § 2 : « Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentementde la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne ale droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ».

[39] *Ibid.*, article 8 § 3 : « Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

[40] Ils n'étendent donc pas le champ d'application du droit de l'Union au-delà de ses compétences : article 51 de la Charte.

[41] *Ibid.*, article 52 § 1.

[42] En la matière, le justiciable pourra se référer utilement au « Manuel de droit européen en matière de protection des données », préparé conjointement par l'Agence des droits fondamentaux de l'Union européenneet le Conseil de l'Europe, en association avec le greffe de la Cour européennedes droits de l'homme, Luxembourg, Office des publications de l'Union européenne, 2014.