Cet article est paru initialement dans la Revue L'Observateur de Bruxelles, Trimestriel d'Informations Européennes, Juillet 2013, n°93

Pour citer cet article : Nathalie Métallinos, « *L'évolution du droit européen en matière de protection des données à caractère personnel et sa pénétration dans les droits nationaux: principes fondateurs et instruments de régulation*», *L'Observateur de Bruxelles*, 07/2013, n°93, p.8-17.

L'évolution du droit européen en matière de protection des données à caractère personnel et sa pénétration dans les droits nationaux: principes fondateurs et instruments de régulation

Nathalie Métallinos

Avocate au barreau de Paris,
Chargée d'enseignement auprès de l'Université Paris II Panthéon-Sorbonne
co-responsable de l'atelier protection des données à caractère personnel de l'ADIJ.

La protection européenne des données à caractère personnel est-elle en bonne santé ? C'est sur cette interrogation qu'un collectif d'auteurs [1] s'est penché fin 2011, sur la capacité de la réglementation européenne à faire face aux défis posés par une société de l'information en constante évolution. Diagnostic : le *patient* a besoin de soins multiples. Notamment, il est apparu aux auteurs que les concepts clés (données à caractère personnel, responsable de traitement) devraient être revisités afin de permettre une protection effective des personnes contre les atteintes à leurs droits et libertés.

Ce constat précède de peu l'annonce par Viviane Reding le 25 janvier 2012 de l'adoption du projet de réforme du cadre européen de la protection des données à caractère personnel (ci-après la Réforme).

Si les grands principes de la protection des données à caractère personnel ne sont pas remis en cause, l'exposé du besoin de réforme exprime la nécessité d'adapter la réglementation existante à la « *protection de la vie privée dans un monde en réseau* »[2] et évoque en arrière-plan l'incohérence et le manque d'effectivité des règles actuelles en raison notamment de l'insuffisance de l'harmonisation dans les Etats membres[3].

Pourtant, le modèle européen de protection des données à caractère personnel est l'un des plus aboutis et ses principes et mécanismes de régulation rayonnent bien au-delà des frontières de l'Europe[4], à tel point qu'il est possible d'affirmer que l'Union européenne exerce un véritable leadership dans ce domaine[5].

Pour pouvoir disposer des clés de lectures nécessaires à la compréhension des enjeux portés par cette réforme, il nous a semblé utile de mettre en perspective le chemin parcouru depuis plus de 30 ans ayant conduit à l'émergence du modèle européen de protection des données à caractère personnel **(I)**, avant d'analyser ses mécanismes de régulation et les limites rencontrées dans l'harmonisation des droits nationaux **(B)**.

---

[1] *S. Gutwirth et al. (Eds.), European Data Protection: In Good Health ?, Springer Science+Business Media B.V., 2012.*

[2] *Protection de la vie privée dans un monde en réseau. Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle, Communication de la commission du 25 janvier 2012, COM(2012) 9 final, p.9.*

[3] *Ibid. p.2.*

[4] *Voir entre autres les travaux de la Conférence Internationale des Commissaires à la Protection des Données et de la Vie Privée et notamment la Résolution de Madrid adoptée lors de la 31ème Conférence en 2009.*

[5] *En ce sens, Abraham L. Newman , "Protectors of privacy. Regulating personal data in the global economy", Cornell University press, 2008.*

I. L'émergence du « modèle européen » : l'affirmation du droit à la protection des données à caractère personnel comme un droit universel

Le droit européen de la protection des données à caractère personnel, désormais encadré par une Directive européenne et consacré en tant que droit fondamental de l'Union européenne, trouve son origine dans les lois nationales adoptés dans les années soixante-dix.

A. Genèse

Les années soixante-dix ont vu l'émergence du droit à la protection des données à caractère personnel en Europe (*Land de Hesse* en 1971*, Suède* en 1973*, France* en 1978) comme rempart contre une évolution non maîtrisée de l'informatique, avec en arrière-plan le spectre de l'évolution vers une société « *Orwellienne* », plusieurs États envisageant d'utiliser l'informatique pour centraliser les grandes bases de données publiques. Le besoin de protection a été grandement renforcé par les scandales ayant ponctué les années soixante et soixante-dix (scandale du *Watergate* aux Etats-Unis, Projet *Safari*[6] et traitement *Gamin*[7] en France) : il s'agissait avant tout de prémunir le citoyen contre les violations des droit et libertés perpétrées par l'État.

La perception de ces menaces, devenue tangible du fait des scandales, a permis l'adoption en Europe[8] de règles strictes et la mise en œuvre de mécanismes de régulation innovants[9]. Ces législations étaient à bien des égards visionnaires : non seulement, en englobant dès l'origine le secteur privé, elles anticipaient sur le développement extraordinaire de la micro-informatique dans l'économie[10], mais aussi, en posant des principes fondamentaux robustes[11], elles ont assuré la continuité des règles reprises dans les divers instruments internationaux.

Ainsi, l'OCDE adopte en 1980 des *Lignes directrices relatives à la protection de la vie privée et les flux transfrontières de données à caractère personnel*[12]. Les *Lignes Directrices*, motivées par les risques que les disparités dans les légalisations nationales n'entravent la libre circulation des données à caractère personnel, constituent le premier instrument international d'harmonisation à ériger en principes fondamentaux les règles relatives à la protection des données personnelles, alors qu'à la date de son adoption, plus de la moitié des États membres de l'OCDE ne disposent pas législation en la matière[13].

La *Convention n°108 du Conseil de l'Europe*[14] est adoptée le 28 janvier 1981 dans un esprit de consécration du droit à protection des données à caractère personnel en tant que droit fondamental, mettant l'accent sur son caractère intangible (les réserves des États membres ne sont pas admises) et le plaçant dans une perspective universelle (la Convention étant ouverte aux pays non membres du Conseil de de l'Europe). A cette date, plusieurs États membres de l'Union européenne

---

[6] *Dans un article intitulé « Safari ou la chasse aux français » (Le Monde, 21 mars 1974), Philippe Boucher révélait un projet secret du gouvernement d'interconnecter les bases de données du secteur public à partir du numéro de sécurité sociale.*

[7] *Un traitement dénommé Gestion Automatisé de la Médecine Infantile (GAMIN) créé dès 1973 dans les centres de protection maternelle et infantile (PMI) prévoyait de pré sélectionner les nourrissons devant faire l'objet de suivi médico-social tout au long de leur scolarité, et ce, à partir de l'analyse automatique des informations figurant sur les certificats de santé. Voir pour plus de détail : CNIL, Les libertés et l'informatique, 20 délibérations commentées, la Documentation Française, 1998.*

[8] *Des législations en matière de protection des données personnelles étaient également adoptées dans d'autres régions du monde (*Australie, Canada, Japon, Etats-Unis*), ces législations présentaient un champ d'application limité (ainsi, le* Privacy Act *américain de 1974, se s'appliquant qu'aux traitements opérés par l'administration fédérale et ne réservant la protection qu'aux seuls citoyens américains), et n'instauraient pas d'organes régulateurs similaires à ceux prévus par les lois européennes.*

[9] *En France, la Commission nationale de l'Informatique et des libertés a été la première « autorité administrative indépendante » et a constitué un modèle de régulation dans tous les secteurs (accès aux documents administratifs (CADA), marchés financiers (AMF, ex-COB), lutte contre les discriminations (Défenseur des droits, ex-HALDE), Énergie (CRE)...*

[10] *Comme le faisait remarquer Guy Braibant en 1998, le premier PC d' IBM a été commercialisé en 1981 (Guy Braibant, Données personnelles et société de l'information, rapport au premier ministre sur la transposition en droit français de la directive 95/46).*

[11] *Etaient identifiés dès l'origine les principes de finalité, loyauté, proportionnalité, droit à l'oubli, interdiction de principe des prises de décision basées sur les profils automatisés, interdiction des transferts vers des pays n'assurant pas un niveau de protection suffisant…*

[12] Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, Recommandation, OCDE, 23 septebre1980.*

[13] *La préface des* Lignes Directrices *mentionne que seuls neuf États membres de l'OCDE disposent déjà d'une législation : l'Allemagne, l'Autriche, le Canada, le Danemark, les États-Unis, la France, le Luxembourg, la Norvège et la Suède. Des projets existent dans quatre États membres de l'OCDE : Belgique, Espagne, Pays-bas et Suisse.*

[14] *Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, n°108, Conseil de l'Europe, 28 janvier 1981.*

reconnaissaient déjà comme un principe à valeur constitutionnelle la protection des données à caractère personnel[15].

En dépit du consensus sur les principes fondateurs, quinze années ont été nécessaires pour l'adoption de la Directive européenne 95/46/CE [16] (ci-après Directive 95/46) fixant un *cadre européen harmonisé* en matière de protection des données à caractère personnel dans un objectif de libre circulation des données au sein des États membres. L'objectif de la Directive est d'assurer un « *niveau de protection équivalent* » des droits et libertés des personnes à l'égard du traitement de ces données dans tous les États membres[17] supérieur à celui de la Convention 108[18]. La Directive 95/46 laisse cependant une large manœuvre d'appréciation aux États membres qui « *pourront donc préciser, dans leur législation nationale, les conditions générales de licéité du traitement des données »*[19], ce qui, en dépit de l'objectif d'harmonisation, a conduit à d'importantes disparités de transposition par les États membres[20]. La Directive 95/46 a été transposée dans les 27 États membres de l'Union européenne[21]. Ces États disposent ainsi tous d'une législation complète en matière de protection des données, reprenant les définitions et principes définis dans la Directive, et ont instauré des autorités de contrôle indépendantes chargées de veiller à l'application de la loi.

La Directive 95/46 n'est pas le seul instrument juridique applicable au traitement de donnée à caractère personnel. Des règles sectorielles ou spécifiques ayant été définies, comme dans le secteur des télécommunications, la Directive Vie privée et communications électroniques[22] ou, dans le domaine de la coopération policière et judiciaire en matière pénale (ancien « troisième pilier »), la décision-cadre 2008/977/JAI3[23].

De plus, complétant le paysage européen de la protection des données personnelles, le règlement européen 45/2001 du 18 décembre 2000 [24] prévoit des dispositions visant à assurer la protection des données à caractère personnel traitées par les institutions et les organes de l'Union européenne et instaurant une autorité de contrôle indépendante, le Contrôleur européen à la protection des données (CEPD), semblable aux autorité nationales mises en place conformément à la directive 95/46.

Cette accumulation de textes européens, décuplée par l'adoption des lois nationales de transposition, a entraîné un morcellement du droit européen de la protection des données personnelles peu propice à une harmonisation totale, ce qui constitue une des raisons de la Réforme en cours.

B. La consécration du droit à la protection des données à caractère personnel en tant que droit fondamental de l'Union européenne

L'ancrage du principe de la protection des données à caractère personnel dans la sphère des libertés publiques et droits fondamentaux est présente dans la Convention 108[25] et dans la directive 95/46 laquelle se réfère à l'article 8 de la Convention européenne des droits de l'homme. Le considérant (10) énonce en effet que « *l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit*

---

[15] Par exemple : Suède (Constitution du 1 janvier 1975, chapitre 2– article 3) ; Portugal (Constitution du 2 avril 1976, article 35) ; Espagne (Constitution du 9 décembre 1978, confirmé par la suite comme un « droit à l'auto-détermination informative » au visa de l'article 18 de la Constitution, Trib. Const. esp., 30 novembre 2000 ».).la France et l'Allemagne verront ce principe consacré par la jurisprudence constitutionnelle Allemagne (droit à l' « auto détermination de la personnalité » trouvant son fondement dans l'article 2 (1) de la Constitution, Trib. Const. Féd., 15 décembre 1983) ; France (référence aux « dispositions protectrices de la liberté individuelle prévues par la législation relative à l'informatique, aux fichiers et aux libertés », Cons. Const., 13 août 1993, Maîtrise de l'immigration).

[16] Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnelle et à la libre circulation de ces données.

[17] Ibid, Considérants (8) et (9) de la Directive 95/46.

[18] Ibid, Considérant (11).

[19] Ibid, Considérant (9).

[20] V. infra II.

[21] La Directive 95/46 s'applique également aux trois pays membres de l'AELE (Islande, Norvège, Lichtenstein,) l'ayant transposée dans leur législation.

[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 qui a remplacé la Directive 97/66/CE du 15 décembre 1997.

[23] 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.

[24] RÈGLEMENT (CE) No 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.

[25] Cf. rapport explicatif précédant le texte de la Convention 108 du Conseil de l'Europe.

à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire; que, pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté ».

Tant la jurisprudence de la Cour européenne des droits de l'homme, que celle de la Cour de Justice de l'Union Européenne, ont intégré la protection des données à caractère personnel dans le principe de protection de la vie privée consacré par l'article 8 de la Convention européenne des droits de l'homme. La jurisprudence de la CEDH, à laquelle les arrêts de la CJUE renvoient[26], fait en effet une interprétation extensive de la notion de protection des données à caractère personnel, lui reconnaissant un rôle fondamental dans la protection de la vie privée[27], et établissant expressément une concordance avec la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981[28].

Consacrant la jurisprudence européenne, la Charte des droits fondamentaux du 7 décembre 2000 a érigé la protection des données à caractère personnel en droit fondamental de l'Union européenne. L'entrée en vigueur du Traité de Lisbonne a eu pour effet de rendre les dispositions de la Charte juridiquement contraignantes[29] et de créer une base juridique spécifique pour l'adoption de règles en matière de protection des données à caractère personnel[30].

II. Le contenu et l'évolution du droit européen de la protection des données personnelles

Avant de présenter les instruments de régulation adoptés et d'évoquer les difficultés d'application, il apparaît pertinent de rappeler de manière synthétique les grands principes dégagés par la Directive 95/46.

A. Fondements légaux et conditions de licéité des traitements

L'article 7 de la Directive a fixé les conditions de légitimité des traitements prévu par l'art.7 de la Directive 95/46). Ainsi, un traitement de données à caractère personnel ne peut être mis en œuvre que sur l'un des fondements suivants : le responsable de traitement a obtenu le consentement *indubitable* de la personne concernée, ou le traitement répond à une exigence de nécessité imputable au responsable de traitement découlant de l'un des éléments suivants: l'application d'une obligation légale, la sauvegarde de la vie de la personne concernée, l'exécution d'une mission de service public ou relevant de l'exercice de l'autorité publique, l'exécution d'un contrat ou de mesures précontractuelles prises à la demande de la personne concernée, et enfin la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

L'application des dispositions de l'article 7 a donné lieu à de nombreuses difficultés d'application, ainsi que l'illustre l'arrêt rendu par la CJUE le 24 novembre 2011[31]. Dans une affaire, la CJUE a rappelé que les États membres ne pouvaient pas soumettre la mise en œuvre d'un traitement à des exigences supplémentaires à celles fixées à l'article 7 de la Directive (cas de la loi espagnole qui imposait le recueil du consentement des personnes mêmes dans les cas où le traitement était nécessaire à la poursuite de l'intérêt légitime du responsable de traitement).

La Directive 95/46 a en outre fixé dans l'article 6 les conditions de licéité devant être respectées par

---

[26] *Par exemple : CJCE, Östericher Rundfunk (c-465/00, C-138/01 et C-139/01) ; CJCE, Volker du 9 novembre 2010 (C 92-09 et C-93-09).*

[27] *CEDH B., G. et M.B. c. France 1 7 décembre 2009, Requêtes n°53354/06, 16425/05, 22115/06).*

[28] *CEDH, Rotaru c. Roumanie, 5 mai 2000.*

[29] *Article 6 (1) du TUE : « L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne (...) laquelle a désormais la même valeur juridique que les traités »*

[30] *Article 16 du TFU : « 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 [politique étrangère et sécurité commune] du traité sur l'Union européenne. »*

[31] CJCE, Asnef, 24 novembre 2011, (Affaires jointes C-468/10 et C-469/10)

les responsables de traitements et les droits des personnes concernées. Ces conditions renforcent les principes contenus dans la Convention 108. Ainsi, une fois le fondement légal du traitement déterminé, le responsable de traitement devra veiller à traiter les données de manière loyale et licite, ce qui implique notamment que les personnes concernées aient reçu une information préalable assurant une collecte loyale des données et que le cas échéant les règles de consentement applicables aient été respectées (*principe de transparence*) et que les finalités du traitement aient été déterminés préalablement, sans qu'il soit possible d'utiliser les données ultérieurement de manière incompatible avec ces finalités (*principe de finalité*).

Par ailleurs, les données collectées doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées (*principe de proportionnalité*) ; exactes et si nécessaire mises à jour et conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (*droit à l'oubli*). Le traitement des données collectées doit de plus être entourés de mesures de sécurité appropriées pour protéger les données contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés ; le recours à la sous-traitance doit être effectué sous l'entier contrôle du responsable de traitement et sous sa seule responsabilité (*confidentialité et sécurité des traitements*).

Des règles spécifiques s'appliquent par ailleurs au traitement des données sensibles, à savoir celles révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, le traitement des données relatives à la santé et à la vie sexuelle, ainsi que celui se rapportant à des infractions pénales, condamnations ou mesures de sûreté (*catégories particulières de données*).

Des garanties importantes sont prévues pour assurer le respect du droit des personnes qui peuvent d'accéder et de se faire communiquer les données à caractère personnel la concernant, ainsi que de connaître à la logique qui sous-tend le traitement automatisé, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive, notamment en raison du caractère incomplet ou inexact des données (*droit d'accès et de rectification*). Les personnes concernées disposent en outre du droit de s'opposer au traitement sous réserve de justifier d'un motif légitime (*droit d'opposition*), celui de s'opposer à utilisation à des fins de prospection commerciale (*droit à la tranquillité*), ainsi que celui de ne pas faire l'objet de décision prises sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de la personnalité (*droit au non ciblage*).

Des règles supplémentaires s'appliquent en cas de transfert des données à caractère personnel en dehors de l'Union européenne (*mise en place des garanties adéquates pour les transferts hors UE*).

Enfin, le responsable de traitement est tenu de respecter les règles liées à l'accomplissement des formalités préalables, et aux contrôles préalables prévues pour les traitements présentant des risques particuliers pour les personnes (*formalités préalables*), plusieurs mesures de simplification étant prévues, dont la possibilité de désigner un délégué à la protection des données, chargé de veiller d'une manière indépendante à l'application des mesures législatives ayant transposé la Directive 95/46.

Pour assurer le respect de ces règles très détaillées et complètes, la Directive 95/46 a prévu un mécanisme de régulation destiné principalement à assurer une application harmonisée.

B. Instruments de régulation

Afin de permettre l'harmonisation de la législation des États membres et la coordination de l'action des autorités nationales, un groupe de travail, le « Groupe de travail de l'article 29 » (G29), a été créé par l'article 29 de la Directive. Le groupe de l'article 29 dispose d'un large pouvoir d'initiative pour contribuer à la mise en œuvre homogène de la Directive 95/46 par les États membres[32] et émettre des recommandations sur « *toute question concernant la protection des personnes à l'égard*

[32] *Dir. 95/46,* Art.30, 1.

du traitement de leurs données à caractère personnel dans la Communauté »[33].

Du fait de son indépendance statutaire[34], de son expertise reconnue et du caractère très innovant de ce mécanisme de gouvernance[35], le G29 a acquis une importance considérable dans l'élaboration des normes européennes de la protection des données à caractère personnel[36] , notamment au travers de ses avis et recommandations. Bien que les documents adoptés par le G29 n'aient pas de valeur contraignante[37], ils font, en général[38], autorité.

Plusieurs avis du G29 sont ainsi venus préciser le champ d'application et les principes clés de la directive n°95/46 tels la loi applicable, l'information préalable des personnes, les concepts de données personnelles, de responsable de traitement et de sous-traitant, de consentement, et de finalité[39].

Le G29 n'est pas le seul acteur à jouer un rôle important dans l'élaboration et l'évolution du droit européen. Ainsi, bien que statutairement le CEPD ne soit compétent que pour veiller à la bonne exécution des dispositions relatives à la protection des données par les institutions et les organes de l'UE, le CEPD a en réalité une influence considérable, en raison (i) de son rôle de conseil auprès des institutions européennes, (ii) de la possibilité qui lui est donnée d'intervenir dans des affaires portées devant les juridictions européennes, et (iii) des positions adoptées, y compris sur des textes ne relevant pas directement de son champ de compétence. Par ailleurs, du fait de l'intensité de son activité[40] et sa réactivité[41], de sa collaboration active avec le G29, le CEPD est largement perçu comme devant jouer un rôle prépondérant dans le nouveau cadre européen de la protection des données personnelles.

C. Les difficultés d'application des règles posées par la Directive européenne 95/46

Bien que l'objectif annoncé de la Directive 95/46 était d'assurer l'harmonisation des règles européennes en matière de protection des données personnelles, et nonobstant les positions adoptées par la jurisprudence européenne ou le G29, des différences importantes existent dans l'application des règles européennes par les États membres, tant du fait de différences de transposition, que de divergences dans l'appréciation du champ d'application de la Directive 95/46.

Nous nous attacherons ci-après à présenter les définitions et grands principes posés par la Directive 95/46 en mettant en lumière, au travers de quelques exemples[42], les difficultés rencontrées dans leur application uniforme par les États membres.

1) Interprétation de la notion de traitement de données à caractère personnel : l'appréhension nuancée du risque de ré identification

Les règles posées par la Directive 95/45 s'appliquent au traitement de données à caractère personnel, qu'il soit automatisé ou non, réalisé par les personnes et organisme privés ou publics établis sur le

---

[33] *Dir. 95/46,* Art.30, 3.

[34] L'article 29, 1 dispose que le G29 « agit de manière indépendante ». Le considérant 65 de la Directive 95/46 fait de cette indépendance une « spécificité » justifiant son rôle de conseil de la Commission européenne et son rôle dans l'harmonisation des règles en matière de protection des données à caractère personnel au niveau communautaire.

[35] *Pour une analyse du rôle du G 29, voir notamment* Yves Poullet et Serge Gutwirth, « The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'? », in Maria Véronica Perez Asinari & Pablo Palazzi (Editeurs), Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law, Bruxelles, Bruylant, 2008, pp570-610.

[36] *Comme par exemple la reconnaissance des règles internes d'entreprises ou Binding Corporate Rules en tant que fondement légal des transferts de données en dehors de l'Union européenne, alors que ce mécanisme n'est pas prévu dans la Directive.*

[37] *L'article 29, 1. de la Directive 95/46 indique que le groupe a un caractère « consultatif ».*

[38] *L'interprétation très extensive de la notion de données personnelles par le G29 (WP n°136) se heurte par exemple à la résistance des acteurs économiques et juridictions au Royaume-Uni en raison de la persistance d'une jurisprudence ayant défini de manière plus restrictive la notion de données à caractère personnelles dans l'affaire "Durant"(Court of Appeal in Durant v Financial Services Authority [2003] EWCA Civ 1746)*

[39] Les documents adoptés par le G29 sont disponibles sur les pages dédiées au G29 du site Europa : *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*.

[40] *Le rapport d'activité 2012 fait état de plus de 33 avis, 42 commentaires rendus en 2012, sans compter le travail d'examen préalable des traitements mis en œuvre par les instances communautaires,*

[41] *L'EDPS a rendu un avis sur le paquet de réforme du cadre européen publié en janvier moins de deux mois après sa publication officielle. .*

[42] *La Commission européenne a conduit une étude comparative en 2010 mettant en évidence ces difficultés dans leur ensemble : Commission Européenne Direction Générale Justice, Liberté et Sécurité, Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques, rapport final, 20 janvier 2010, accessible en ligne sur : http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf*

territoire de l'Union européenne ou ayant recours à des moyens de traitement dans l'Union européenne.

Les notions de *traitement* et de *données à caractère personnel* sont définies et interprétées[43] de manière très large de telle sorte que relèvent du champ d'application des règles posées par la Directive tout utilisation ou autre forme de manipulation[44] de données permettant d'identifier une personne physique ou simplement *pouvant être reliées à une personne physique*[45], impliquant un lien avec une personne physique, réalisé par des moyens informatiques ou contenus dans un fichier[46].

La jurisprudence européenne a consacré une interprétation extensive de cette définition laquelle s'applique indifféremment aux activités professionnelles[47], à des données déjà rendues publiques[48], à une liste de participants (nom et prénoms) à une réunion[49], aux revenus de personnes[50] et inclut les empreintes digitales et les profils ADN[51], ainsi que l'adresse IP (dès lors qu'elles permettent l'identification précise des utilisateurs[52]).

Le groupe de l'article 29 a quant à lui étendu la notion de données à caractère personnel à des données telles que l'adresse MAC enregistrée sur des composants matériels informatiques[53], des données de localisation dans le cadre de la fourniture de services de communications électroniques publics[54], le « diagramme unique de charge énergétique » d'un compteur intelligent ou encore « les métadonnées se rapportant à la configuration du compteur intelligent »[55].

Nonobstant cette interprétation très extensive du champ d'application matériel, le concept de données à caractère personnel est encore discuté et des divergences subsistent, parfois importantes, au niveau des États membres, tant au regard des positions adoptés par les autorités de protection des données, que de celles de la jurisprudence nationale. Ces divergences résultent principalement d'interprétations divergentes de la force du « lien » devant exister entre une donnée et une personne physique pour que cette dernière puisse être qualifiée de données à caractère personnel ou autrement dit de la détention par les responsables de traitement de la « clé » de concordance permettant d'associer une donnée à une personne physique[56]. Bien que les Considérants 26 et 27 de la Directive 95/46 invitent à retenir comme limite le caractère *raisonnable* des moyens d'identification susceptibles d'être mis en œuvre pour identifier la personne concernée, cet élément de modération a été transposé différemment dans les législation des États membres.

Certaines législations ont retenu comme élément d'atténuation le fait qu'il ne soit pas possible d'identifier une personne physique « par des moyens légaux » (Autriche) ou encore le caractère « probable » de l'identification par le responsable de traitement (Royaume-Uni). En France, la référence à « l'ensemble des moyens d'identification susceptibles d'être mis en œuvre », amputée de l'adverbe raisonnablement, a eu l'effet inverse : pour la CNIL, il suffit que l'identification soit possible, quelle que soit l'importance des moyens mis en œuvre par le responsable de traitement pour y parvenir.

Par ailleurs, la jurisprudence nationale est parfois allée à l'encontre même de la loi, retenant une

---

[43] Voir notamment les avis du Groupe de l'article 29 sur le concept de données à caractère personnel

[44] Dir. 95/46, art. 2, b., « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés (...) telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction».

[45] Avis 4/2007 du Groupe de travail de l'article 29 sur le concept de données à caractère personnel adopté le 20 juin 2007.

[46] Dir. 95/46 – art. 2,c., "tout ensemble structuré et stable accessible selon des critères déterminés que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

[47] CJCE Volker, op. cité.

[48] Données déjà publiées dans les médias, CJCE 16/12/2008 Tietosujavaltuutettu.

[49] CJUE 26/06/2010 Commission c. Bavarian lager.

[50] Pour des revenus alloués à des agents publics, CJCE Österreichischer Rundfunk op. cité.

[51] CEDH 4/12/2008 Marper c/ Royaume-Uni

[52] CJUE 24/11/2011 Scarlet (et CJCE 26/01/2008 Promusicae).

[53] G 29, WP 185.

[54] Ibid.

[55] G 29, WP 183.

[56] Étude comparative, op., citée p.55.

conception extrêmement restrictive de la notion de données à caractère personnel : tel a été le cas du Royaume-Uni où la célèbre (et controversée) affaire Durant c/FSA dans laquelle la Court of Appeal a considéré aux termes d'une analyse sémantique que la notion de donnée relative à une personne physique devait être interprétée comme *se référant à*, au sens de *caractérisant*, et donc *affectant sa vie privée* (et non *ayant un lien avec*) [57].

Ces quelques exemples illustrent la complexité de fixer une limite entre *données à caractère personnelles* et *données anonymes*, cette distinction étant au cœur de l'application de la législation, et donc de la révision du cadre européen. Or le développement des capacités de ré identification, par exemple en raison du nombre de traces laissées par l'usage d'Internet des outils connectés ou des capacités d'association générées par la disponibilité accrue des données (*Open data* et *Big data*), montre la quasi-impossibilité de rendre les données à caractère personnel définitivement anonymes et est, à juste titre, identifié comme l'un des plus grands défis en matière de protection des données[58].

2) Les difficultés et enjeux tenant à la définition de la loi applicable et à la responsabilité des traitements

La Directive 95/46 a défini plusieurs critères destinés à déterminer les cas où un traitement de données à caractère personnel sera concerné par la réglementation. Ainsi, tel sera le cas si le responsable de traitement dispose d'un établissement sur le territoire d'un État membre, ou si, sans être établi sur le territoire de l'Union européenne, il a recourt à des « moyens » automatisés ou non, situés sur le territoire d'un État membre[59]. En cas d'établissement dans plusieurs États membres, la Directive prévoit que le traitement doit respecter chacun des droits nationaux applicables.

Le second critère de compétence territoriale retenu, dans le cas où le responsable de traitement n'est pas présent sur le territoire de l'Union européenne, n'est pas défini dans la Directive 95/46. De plus, une divergence d'interprétation apparaît entre la version anglaise qui utilise le terme d' « *équipement* » (c'est-à-dire « *matériel* », par exemple un périphérique, un appareil), alors que d'autres versions (par exemple allemande, grecque, espagnole, portugaise) utilisent la notion plus large de « *moyens* » (« *instrument* » pour la version italienne). Le G29 retient une interprétation large de la notion de moyens en considérant dans ses avis qu'un cookie constitue un « *moyen* » visé à l'article 4[60].

Par ailleurs, pour pouvoir déterminer la loi applicable, encore faut-il identifier le responsable de traitement. Le responsable de traitement est « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel*[61] *».* Le responsable de traitement se distingue du « *sous-traitant* » en ce que cette notion désigne la « *personne physique ou morale, autorité, organisme, service traitant les données pour le compte du responsable de traitement».*

Ces qualifications sont au cœur du système de responsabilité établi par la Directive 95/46 dans la mesure où le responsable de traitement est celui qui est responsable des diverses obligations prévues par la Directive et que sa détermination permet également de déterminer la loi applicable. Il est entendu que pour retenir la qualification de responsable de traitement, il est nécessaire de retenir les critères de définition de la finalité et des moyens de manière cumulative. Le G29 dans un avis rendu en 2010, tout en reconnaissant les difficultés visées par cette distinction et les responsabilités associées, invite à une approche pragmatique mettant davantage l'accent sur le pouvoir discrétionnaire de déterminer les finalités et sur la latitude laissée pour prendre des décisions, pour conclure que « *Si un contractant avait une influence sur la finalité et qu'il procédait au traitement (également) à des fins personnelles, par exemple en utilisant les données à caractère personnel*

---

[57] *2003] EWCA Civ 1746. Pour une analyse, voir par exemple : Lilian Edwards, Taking the "Personal" Out of Personal Data: Durant v FSA and its Impact on the Legal Regulation of CCTV, SCRIPT-ED, Volume 1, Issue 2, June 2004, p. 85-93, accessible en ligne : http://www.law.ed.ac.uk/ahrc/script-ed/issue2/durant.asp*

[58] *Étude comparative, op. citée p.34.*

[59] *Les traitements réalisés à des fins de transits sont exclus du champ d'application de la Directive*

[60] *G29, WP 56 et WP 148*

[61] *Dir. 95/46 - art. 2, d.*

reçues en vue de créer des services à valeur ajoutée, il deviendrait alors responsable du traitement (ou éventuellement co-responsable du traitement) pour une autre activité de traitement et serait donc soumis à toutes les obligations prévues par la législation applicable en matière de protection des données.[62] »

Le projet de règlement européen vise incontestablement à tenir compte de cette difficulté notamment au regard des nouvelles offres de services (par exemple les solutions de « *cloud computing* ») où la répartition classique des rôles et responsabilités est discutable, notamment compte tenu de l'autonomie dont jouit le prestataire dans la définition, non seulement des moyens (techniques et organisationnels) mais aussi des finalités (par exemple le transfert de données en dehors de l'Union Européenne à des fins d'hébergement.

Par ailleurs, s'agissant des règles de compétente territoriale, la référence aux traitements effectués *dans le cadre d'un établissement* situé dans le territoire de l'Union Européenne, et non pas simplement du lieu d'établissement du responsable de traitement (qui aurait pu renvoyer à la notion « d'établissement principal »[63]), a pour effet de désigner, en plus de l'établissement principal, tous les établissement secondaires. Le considérant 19 de la Directive 95/46 est d'ailleurs venu préciser la notion d'établissement comme visant *tout* type d'établissement, indépendamment de la forme juridique, dès lors qu'il suppose l'exercice d'une activité effective au moyen d'une « installation stable ». Sont donc visées non seulement les filiales, mais aussi les succursales, les bureaux, la présence d'un seul salarié exerçant une activité pouvant suffire.

Le critère principal retenu, en multipliant les fors de compétence, et donc le nombre de formalités alourdit considérablement les démarches devant être effectuées par un responsable de traitement disposant d'établissements dans plusieurs États membre, compte tenu des disparités plus qu'importantes en la matière[64], et ce d'autant qu'une telle solution présume que tous les « établissements » (succursale, bureau, salarié) ont la qualité de responsable de traitement, ce qui n'est pas toujours le cas, notamment pour des traitements mis en œuvre de manière globale. Cette multiplication a également pour effet d'accroître les risques d'interprétation divergente sur un même traitement mis en œuvre de manière concomitante sur tout le territoire de l'UE.

*

* *

Si en principe, une harmonisation des règles aurait dû conduire à neutraliser ces effets multiplicateurs, et aussi à rendre inutiles toute stratégie de *forum shopping,* en réalité les enjeux sont considérables pour les responsables de traitement, notamment en raison de l'existence dans certains États membre de régimes d'autorisation, plus ou moins complexes, occasionnant des délais d'instruction et parfois des incertitudes sur l'issue de la demande d'autorisation.

Ce rapide tour d'horizon permet d'illustrer l'extrême complexité d'une application uniforme des règles déterminées par la Directive 95/46 en matière de protection des données à caractère personnel et ce alors qu'un consensus fort existe sur l'application de principes ancrés dans les libertés publiques et que l'Union européenne a su mettre en œuvre des mécanismes de régulation innovants. Ce faisant, il est possible de mesurer l'ampleur des attentes liées à la réforme du cadre européen en la matière, qui devra, tout en précisant d'avantage les concepts et critères, assurer la cohérence propre à garantir une sécurité juridique dans la mise en œuvre des traitements, tout en n'abaissant pas le niveau de protection des individus.

---

[62] *G 29, WP 169, p.15.*

[63] *En ce sens, Lokke Moerel « Back to basics » :when does EU data protection law apply ?, International Data Privacy Law, 2011, Vol. 1, No.2, pp92-110.*

64 A titre d'illustration, la finalité et la mise en œuvre des systèmes d'alerte professionnelle est strictement contrôlée en France du fait de l'existence d'un régime autorisation préalable, alors que dans la plus part des autres Etats membres, ils n'entraînent pas, en soi, de formalités spécifiques, étant englobés dans le traitement de gestion du personnel (comme en Pologne ou en l'Espagne). Un autre exemple contrasté est celui d'usage de dispositifs biométriques dont la mise en œuvre est conditionnée soit à une autorisation législative, comme en Norvège, ou de l'autorité de protection des données personnelles, comme en France ou en Italie, ou à l'inverse n'est soumis qu'à un simple régime de déclaration, comme en Espagne.