Journal de droit européen

Juin 2012
N° 190 — 20e année

Bureau de dépôt: Louvain 1 - Mensuel, sauf juillet/août
P301030

larcier

ISSN 0779-7656 – D 2012/0031/049

Paul NIHOUL, rédacteur en chef

ANALYSE

Proposition de règlement sur la protection des données - Premiers commentaires

Claire Gayrel[1] et Romain Robert[2]

Le Traité de Lisbonne ayant élevé le droit à la protection des données au rang de droit fondamental, la Commission propose une refonte des règles en la matière. Celle-ci consacre le droit à l'oubli et renforce la protection contre le profilage. La suppression du devoir de notification, l'allégement du régime applicable aux P.M.E. et la création de la fonction de délégué à la protection des données sont autant d'innovations proposées.

1
Introduction

La protection de la vie privée et des données à caractère personnel est à l'heure de la révision. Trente ans après son adoption, le Conseil de l'Europe a lancé, début 2011, une consultation publique visant à évaluer la nécessité de procéder à une révision de la Convention 108[3] au vue des nouveaux enjeux et défis technologiques. Cette consultation fut suivie de propositions de modernisation de la Convention qui sont actuellement à l'étude au Comité consultatif de la Convention 108[4]. L'Union européenne s'est quant à elle aussi engagée sur la voie de la révision de ses instruments législatifs, visant ainsi à promouvoir *une approche globale et compréhensive* de la protection des données[5] dans le nouveau cadre du Traité de Lisbonne. Une proposition de règlement et une proposition de directive ont été présentées par la Commission européenne le 25 janvier 2012, destinés à remplacer respectivement la directive 95/46/CE sur la protection des données à caractère personnel[6] et la décision cadre 2008/977/JAI sur la protection des données dans le cadre de la coopération policière et judiciaire[7]. Nous présentons ici les grandes lignes du projet de règlement et commenterons ses dispositions essentielles à l'aune de son objectif de modernisation et laisserons à part nos commentaires sur le projet de directive. Notons d'emblée une évolution perceptible d'orientation du futur instrument : l'effacement de la protection de la vie privée derrière le nouveau droit fondamental à la protection des données. En effet, avec d'autres[8], nous regrettons que l'article 1er du projet de règlement évacue l'objectif de protection de la vie privée et se réfère uniquement de manière explicite à la protection des données à caractère personne[9]. Nous commencerons par analyser les choix de la Commission en termes d'instruments juridiques et les implications de ce choix, pour ensuite passer en revue les changements majeurs résultant de la proposition.

2
Le choix de l'instrument législatif en question

Si le choix de proposer au législateur européen un règlement, à caractère obligatoire et directement applicable dans tous ses éléments, trouve sa justification dans l'objectif de doter l'Union d'un cadre légal harmonisé entre États membres, cette option n'allait pas de soi. En effet, comme le rappelle le Contrôleur européen de protection des données (C.E.P.D.)[10], mais aussi le Groupe de l'Article 29[11], la Commission aurait pu soumettre au législateur un instrument général unique, tant pour la matière commerciale que la matière pénale, sur le modèle de la Convention 108[12]. Une proposition en ce sens aurait consisté en une di-

(1) Chercheuse au C.R.I.D.S. (Centre de recherche information, droit et société), Facultés universitaires Notre-Dame de la Paix (Belgique), claire.gayrel@fundp.ac.be.

(2) Conseiller juridique - Commission de la protection de la vie privée (Belgique). Les propos de l'auteur sont personnels et ne reflètent pas le point de vue de la Commission.

(3) Convention du Conseil de l'Europe n° 108 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981.

(4) Voy. l'ensemble des travaux en cours sur le site du Comité Consultatif de la Convention 108 : http://www.coe.int/t/dghl/standardsetting/dataprotection/Calendar_fr.asp.

(5) Communication de la Commission « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », 4 novembre 2001, COM(2010)609 final.

(6) Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 sur 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.C.E.* L 281 du 23 novembre 1995, ci-après « directive 95/46 ».

(7) 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.U.E.* L 350 du 30 décembre 2008.

(8) Voy. Y. Poullet et L. Costa, « Privacy and the Regulation of 2012 », *Computer Law & Security Report*, vol. 28, issue 3, juin 2012, pp. 254-262.

(9) En contraste avec l'article 1.1 de la directive 95/46 qui prévoit que « [l]es États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, *notamment de leur vie privée*, à l'égard du traitement des données à caractère personnel ». Cet effacement de la vie privée, au fondement du droit à la protection des données, peut être analysé à la lumière de la distinction établie entre ces deux droits dans la charte des droits fondamentaux de l'Union entrée en vigueur avec le Traité de Lisbonne le 1er décembre 2009.

(10) Opinion of the European Data Protection Supervisor on the protection reform package, 7 March 2012, ci-après « Avis du C.E.P.D. du 7 mars 2012 », voy. les points I.2.a. « the data protection framework is only partly covered » et I.2.b. « the two proposed instruments taken together do not create a comprehensive data protection framework », www.edps.europa.eu.

(11) Opinion 01/2012 of Article 29 Data Protection Working Party on the data protection reform proposals adopted on 23 March 2012, p. 5, ci-après « Avis 01/2012 du Groupe de l'Article 29 ».

(12) Ce qui aurait permis de répondre aux critiques concernant la coexistence de multiples instruments de protection des données dans l'Union.

rective générale fixant les objectifs à atteindre, tout en laissant les États membres libres quant à la forme et aux moyens selon la formule consacrée[13]. Il nous apparaît dès lors que le choix de deux instruments prolonge la fragmentation du cadre légal de protection des données en contraste avec l'objectif annoncé d'un cadre *global*, mais aussi comme le laissait entrevoir le Traité de Lisbonne, prolonge la pilarisation du système en matière de protection des données. En effet, la Commission n'a pas exploité la seule base juridique de l'article 16 TFUE pour faire ses propositions de réforme, mais a choisi de prendre en compte les déclarations n^{os} 20 et 21 y annexées[14]. Ainsi le règlement ne s'applique pas aux traitements réalisés dans le cadre de la politique étrangère et de sécurité commune[15] pour lesquels aucune proposition législative n'a été avancée, et bien sûr ceux qui sont réalisés aux fins de prévention, détection, enquêtes, et poursuites d'infractions pénales et d'exécution de sanctions pénales[16] qui sont quant à eux couverts par la proposition de directive.

Le maintien d'un cadre légal fragmenté de protection des données se trouve aussi illustré dans les champs d'application du règlement et de la directive. Ceux-ci ne s'appliquent pas aux activités « n'entrant pas dans le champ d'application du droit de l'Union, en ce qui concerne notamment la sécurité nationale »[17], traitements qui continuent de relever des compétences des États membres, et aux traitements des institutions, organes et organismes de l'Union[18]. Les traitements couverts par l'actuel règlement 45/2001[19], ainsi que ceux couverts par des actes spécifiques de l'Union, en particulier le système d'information Schengen, mais aussi dans le domaine de la coopération policière, Europol, Eurojust ou encore la décision Prüm, restent donc en dehors du règlement et de la directive. Autrement dit, si le règlement contribuera, au moyen de son applicabilité directe, à accroître l'harmonisation des règles de protection des données entre les États membres pour les traitements qu'il couvre, le choix d'un double instrument et leurs nombreuses exclusions ne répondent pas à l'enjeu de la fragmentation du cadre légal.

Par ailleurs, le maintien de deux instruments généraux risque de soulever certaines questions concernant les règles applicables dans certains cas. Si les traitements réalisés par les « autorités nationales compétentes » au sens de la directive aux fins de prévention, détection, enquête et poursuite des infractions pénales et exécution des sanctions pénales seront soumis aux règles nationales transposant la directive, certains traitements réalisés par ces mêmes autorités nationales compétentes relèveront du règlement. Il faudra que les autorités nationales en cause veillent à distinguer clairement les traitements en fonction des règles auxquels ils seront soumis. Cela relève selon nous d'un exercice potentiellement difficile, dès lors qu'il n'est pas exclu qu'un même traitement de données puisse être à la fois soumis au règlement et à la directive.

3

Les champs d'application du règlement

A. — Champ d'application matériel

Outre les exclusions déjà discutées, le règlement ne s'applique pas, comme l'actuelle directive 95/46, aux traitements réalisés par une personne physique dans le cadre de ses activités exclusivement personnelles ou domestiques et lorsqu'ils sont « sans but lucratif ». Cette précision a notamment pour but d'éviter que les traitements tels que ceux faits sur les réseaux sociaux puissent échapper à la législation proposée au motif qu'ils sont réalisés à titre personnel[20].

Par ailleurs, le règlement prévoit la possibilité d'exceptions au respect de certains principes pour certains traitements, en particulier concernant le secteur public. L'article 21 prévoit que des limitations peuvent être apportées par les États membres aux principes cardinaux de la protection des données énoncés à l'article 5 (principe de licéité, de loyauté, transparence, de finalité, de qualité des données, de minimisation, de conservation limitée), ainsi qu'aux droits des personnes concernées et à l'obligation de notification des violations de sécurité lorsqu'elles s'avèrent nécessaires[21]. Ces limitations reprennent largement celles de l'actuel article 13 de la directive 95/46, mais apparaissent aussi plus étendues notamment en ce qui concerne les « autres intérêts généraux de l'Union ou d'un État membre » qui peuvent justifier des limitations au règlement, cantonnés dans la directive actuelle à un « intérêt économique ou financier important »[22].

B. — Champ d'application territorial de la proposition de règlement

L'article 3 de la proposition détermine le champ d'application territorial du règlement. Le premier paragraphe reprend le critère du lieu de l'établissement du responsable du traitement, critère qui avait déjà été retenu dans la directive 95/46[23]. Il confirme que le règlement sera applicable au traitement de données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement de données ou d'un sous-traitant sur le territoire de l'Union. À la différence du libellé de la directive 95/46, l'article 3 du règlement précise qu'il s'appliquera également quand le sous-traitant est établi sur le territoire de l'Union[24]. En l'absence d'établissement du responsable du traitement ou d'un sous-traitant sur le territoire de l'Union européenne (ou dans un lieu où la législation nationale d'un État membre s'applique en vertu du droit international public[25]), le règlement s'appliquera également au traitement de données à caractère personnel de personnes concernées ayant leur résidence sur le territoire de l'Union[26], lorsque les activités de traitement sont soit liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, soit à l'observation de leur comportement.

Le règlement propose donc d'abandonner le critère actuel du recours à des moyens situés sur le territoire d'un État membre, pour préférer deux nouveaux critères plus adaptés à un environnement numérique et transfrontière. Ceux-ci permettront donc au règlement de s'appliquer aux responsables du traitement établis hors de l'Union, notamment lorsque leurs activités s'adressent à des individus résidant dans l'Union, et notamment lorsque ces derniers sont profilés sur Internet[27]. Si la proposition de règlement comporte un effet extraterritorial potentiel, on s'interroge sur son effectivité concernant les responsables du traitement établis hors du territoire de l'Union, à savoir comment les dispositions du règlement et les mesures adoptées par les autorités de protection des données seront mises en œuvre à l'égard de responsables établis en dehors du territoire de l'Union européenne[28].

(13) Définition de la « directive », article 288.3 du Traité sur le fonctionnement de l'Union européenne (TFUE).

(14) Elles prévoient respectivement que « chaque fois que doivent être adoptées, sur la base de l'article 16, des règles[...] qui pourraient avoir une incidence directe sur la sécurité nationale, il devra en être dûment tenu compte » (déclaration n^{o} 20), tandis que « des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 du TFUE pourraient s'avérer nécessaires » (déclaration n^{o} 21).

(15) Article 2.2, c), de la proposition de règlement.

(16) Article 2.2, e), de la proposition de règlement.

(17) Article 2.2, a), de la proposition de règlement et article 2.3, a), de la proposition de directive.

(18) Article 2.2, b), de la proposition de règlement et article 2.3, b), de la proposition de directive.

(19) Règlement (CE) n^{o} 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.C.E.* L 8 du 12 janvier 2001.

(20) Ce souci avait été soulevé par le Groupe de l'Article 29 dans son document « L'avenir de la protection de la vie privée » du 1er décembre 2009, WP 168, point 71, et dans son avis 5/2009 du 12 juin 2009 sur les réseaux sociaux en ligne, WP 163. Voy. également l'arrêt de la C.J.C.E., *Satamedia*, du 16 décembre 2008, C-73/07, § 44 où la Cour a considéré que l'exception de l'article 3.2 de la directive 95/46 ne s'appliquait pas aux activités de sociétés dont l'objet est de porter les données collectées à la connaissance d'un nombre indéfini de personnes.

(21) Ainsi, « la sécurité publique » la sauvegarde « d'autres intérêts généraux de l'Union ou d'un État membre », « la prévention et la détection de manquements à la déontologie des professions réglementées, l'accomplissement de missions de contrôle, d'inspection ou de réglementation liée « même occasionnellement », à l'exercice de l'autorité publique, et « la protection de la personne concernée ou des droits et libertés d'autrui » peuvent servir de fondement législatif à des restrictions au respect du règlement selon l'article 21, a) à f), de la proposition de règlement.

(22) Article 13.1, e), de la directive 95/46.

(23) Article 4.1 de la directive 95/46.

(24) L'article 4.1, a), de la directive 95/46 pouvait toutefois conduire à la même conclusion dès lors qu'en l'absence d'établissement du responsable du traitement sur le territoire d'un État membre, l'utilisation de moyens situés sur leur territoire pouvait entraîner l'application de la directive. L'appel à un sous-traitant pour réaliser des opérations sur des données pouvait donc s'assimiler à l'utilisation de moyens sur le territoire d'un État membre.

(25) Article 4.3 de la proposition de règlement.

(26) Il est permis de s'interroger sur l'opportunité du critère de résidence des personnes concernées pour la détermination du champ d'application territorial du règlement dans certaines hypothèses, excluant dès lors la protection de personnes non résidentes présentes sur le territoire de l'UE, tandis que la directive 95/46 actuelle, mais plus généralement la protection des droits fondamentaux octroyés par la Convention européenne des droits de l'homme, et en particulier son article 8, est accordée à toute personne, en dehors de tout critère de nationalité ou de résidence.

(27) Voy. considérant 21 de la proposition de règlement.

(28) Voy. les doutes exprimés par le UK Information Commissioner's Office : *Initial analysis of the European Commission's proposal for a revised data protection legislative framework*, 27 février 2012, www.ico.gov.uk, p. 5 : « The Regulation should be realistic about this and should not lead EU consumers to believe that the law offers them a degree of protection that, in reality, it cannot deliver ».

4

Principes et définitions : quelques évolutions

Nous proposons de relever ici, quelques définitions et principes qui existaient déjà dans la directive 95/46, mais qui connaissent une évolution dans la proposition étudiée.

A. — Le concept de donnée à caractère personnel

Une donnée à caractère personnel, concept clé de la directive 95/46, est désormais définie comme « toute information se rapportant à une personne concernée »[29]. Tous les éléments qui définissaient une donnée à caractère personnel dans la directive 95/46 sont repris dans la définition de « personne concernée ». Ces éléments sont les mêmes, sauf l'ajout des références aux données de localisation ou d'identifiants en ligne.

On peut lire cette modification de perspective des définitions à la lumière de l'objectif général de la proposition, qui est d'élever la protection accordée aux individus concernant leurs données. Ainsi, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement, mais aussi par toute autre personne[30].

Ceci reflète, d'une part, le souci de protéger les données d'individus qui ne sont pas identifiés nominativement d'autre part, les conclusions de l'avis du Groupe de l'Article 29 qui considérait qu'une personne devenait identifiable lorsqu'on pouvait la distinguer d'autres personnes du groupe et par conséquent la traiter différemment[31]. Les *cookies*, adresses IP et autres identifiants non nominatifs, lorsqu'ils influencent ou déterminent la manière dont une personne est traitée ou évaluée (et permettent, par exemple, le profilage ou la publicité comportementale en ligne), peuvent donc à notre sens être assimilés à des données à caractère personnel et donc entraîner l'application du règlement[32].

B. — Principes relatifs au traitement

L'article 5 de la proposition de règlement reprend à peu de choses près les mêmes principes cardinaux que ceux posés par l'article 6 de la directive 95/46. Notons toutefois que l'article 5, c), de la proposition renforce et explicite le principe de minimisation des données, en exigeant du responsable qu'il ne traite des données à caractère personnel que si cela est strictement nécessaire pour la finalité du traitement. En outre, l'article 5, f), pose le principe de responsabilisation *(accountability)*, explicité *infra* dans la présente contribution.

C. — Bases de légitimité de traitement

L'article 6 de la proposition apporte quelques changements aux bases de légitimité sur lesquelles doit reposer tout traitement de données[33]. Ainsi, il est spécifié que les traitements effectués pour le respect d'une obligation légale ou en vertu d'une mission d'intérêt général ou relevant de l'exercice de l'autorité publique doivent trouver leur fondement juridique dans le droit de l'Union ou d'un État membre auquel le responsable du traitement est soumis[34]. On constate donc que l'application d'une loi non européenne est exclue en tant que base légale fondant la légitimité[35]. Notons également que l'article 6.1, f) de la proposition de règlement, qui permet un traitement à la condition de réaliser une balance des intérêts en présence, ne sera pas applicable aux traitements effectués par les autorités publiques[36].

Enfin, avec le C.E.P.D.[37], nous regrettons que l'article 6.4 introduise une entorse au principe d'interdiction de détournement de finalité, en prévoyant que la finalité d'un traitement ultérieur peut reposer sur l'une des bases de légitimité de l'article 6.1, a) à e)[38].

D. — Le consentement

Notons que la proposition de règlement précise la notion de consentement comme « toute manifestement de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[39]. L'article 7 de la proposition renforce également les conditions du consentement[40] en mettant la charge de la preuve de l'obtention de ce dernier sur le responsable du traitement, en exigeant que ce consentement soit exprimé de manière distincte[41], en permettant qu'il soit retiré à tout moment, et en considérant que le consentement ne peut constituer un fondement juridique valable pour le traitement lorsqu'il existe un déséquilibre significatif entre la personne concernée et le responsable de traitement[42].

5

Les principes et concepts nouveaux

Sans être exhaustifs, nous retenons ci-dessous les principes et concepts nouveaux introduits par la proposition de règlement qui méritent selon nous d'être soulignés.

A. — La protection des enfants et des mineurs

L'article 8 de la proposition renforce la protection des enfants, dans le cadre d'offres de services de la société de l'information, et dispose que les mineurs de moins de 13 ans ne peuvent valablement consentir au traitement de leurs données sans l'autorisation ou le consentement d'un parent de l'enfant ou d'une personne qui en a la garde[43]. La Commission dispose du pouvoir d'adopter des actes délégués pour préciser les méthodes permettant de s'assurer du consentement des mineurs[44].

B. — Nouvelles définitions

La proposition de règlement introduit, en son article 4, quelques nouvelles définitions, comme la notion de « violation des données à caractère personnel », les notions de « données génétiques », de « données biométriques », et de « données concernant la santé », de « représentant », d'« entreprise », de « groupe d'entreprises », de « règles d'entreprises contraignantes », ou encore d'« enfant », défini comme toute personne âgée de moins de 18 ans.

Notons également l'introduction du concept d'« établissement principal »[45], défini, pour ce qui concerne le responsable de traitement, comme « le lieu de son établissement dans l'Union où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère

(29) Article 4 (2) de la proposition de règlement.
(30) Article 4 (1) et considérant n° 23 de la proposition de règlement.
(31) Avis 4/2007 du Groupe de l'Article 29 du 20 juin 2007 sur le concept de données à caractère personnel, WP 136, p. 10.
(32) Remarquons que le considérant n° 24 de la proposition de règlement maintient une ambiguïté d'interprétation dès lors qu'il affirme que les identifiants en ligne ne doivent pas être automatiquement considérés comme des données à caractère personnel. Le Groupe de l'Article 29, dans son avis n° 01/2012 appelle d'ailleurs à une clarification de cette définition.
(33) Ces bases étant fixées par l'article 7 de la directive 95/46.
(34) Article 6.3 de la proposition de règlement.
(35) Ainsi une loi américaine, comme la loi *Sarbane-Oxley*, ne pourrait pas constituer une telle base légale.
(36) La Commission pourra d'ailleurs adopter des actes délégués en conformité avec l'article 86 pour préciser les conditions de cette balance : voy. article 6.5 de la proposition de règlement.
(37) Avis du C.E.P.D. du 7 mars 2012, §§ 120-124, pp. 21-21.
(38) Ceci signifie par exemple qu'une loi pourra rendre légitime un traitement ultérieur *a priori* incompatible.
(39) Article 4 (8) de la proposition de règlement.
(40) Cette nouvelle approche des conditions entourant le consentement s'inspire des conclusions de l'avis du Groupe de l'Article 29 n° 15/2011 sur le consentement du 13 juillet 2011, WP 187.
(41) Le considérant 25 de la proposition de règlement explicite ces principes en disposant par exemple que le consentement donné sur internet devra être spécifique et donné par exemple en cliquant une case.
(42) Le considérant 34 cite les exemples de données de travailleurs traitées par l'employeur dans le cadre de relations de travail, ou de données traitées par une autorité publique.
(43) On remarque que le règlement entend donc régler une question qui s'apparente généralement au droit des personnes, et plus spécifiquement à la capacité juridique des mineurs à consentir à certains actes juridiques, même si l'article 8.2 avance que ce principe n'affecte pas la législation générale des États membres en matière contractuelle, comme les dispositions régissant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.
(44) On peut bien sûr penser à l'utilisation de la carte d'identité électronique dans les États membres où une telle carte existe. On veillera toutefois à préserver le droit à l'anonymat des utilisateurs mineurs qui ne devraient à notre sens pas être identifiés par l'utilisation de ces moyens techniques. Voy. en ce sens, recommandation 3/97 du Groupe de l'Article 29 du 3 décembre 1997, « L'anonymat sur Internet », WP 6.
(45) Article 4 (13) de la proposition de règlement.

personnel; si aucune décision de ce type n'est prise dans l'Union, l'établissement principal est le lieu où sont exercées les principales activités de traitement dans le cadre des activités d'un établissement du responsable du traitement dans l'Union ». Ce critère, même explicité par le considérant 27, ne nous semble pas aisé à appliquer. On comprend que le texte souhaite prendre en considération non pas le lieu où se prennent les décisions relatives à l'activité principale de l'entreprise (traditionnellement et généralement son siège social central dans l'Union européenne), mais plutôt le lieu où les décisions concernant le traitement en cause sont adoptées[46], sans que cet État membre soit forcément celui où les moyens techniques pour le traitement sont déployés. Le C.E.P.D. a déploré la difficulté d'application de ces critères[47], tout comme le Groupe de l'Article 29[48], dans le cas où un groupe ayant plusieurs filiales dans l'Union procède à un ou plusieurs traitements. Cette question est fondamentale dès lors que c'est le lieu de l'établissement principal d'un groupe qui déterminera l'autorité de protection des données compétente en vertu de l'article 51.2 de la proposition de règlement.

L'article 4 (13) de la proposition de règlement précise qu'en ce qui concerne les sous-traitants, on entendra par établissement principal le lieu de son administration centrale dans l'Union. Le critère est donc différent de celui retenu pour déterminer le lieu d'établissement principal des responsables du traitement.

C. — Principes de *privacy by design* et de *privacy by default*

L'article 23 de la proposition de règlement consacre les principes de *privacy by design* (« protection des données dès la conception ») et de *privacy by default* (« protection des données par défaut »). Ainsi, l'article 23.1 prévoit que « le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée ». Il s'agit du principe de *privacy by design*, qui imposera donc au responsable de traitement d'implémenter dans les mesures techniques des services et des produits qui offrent des solutions permettant de respecter les principes posés par la réglementation de protection des données à caractère personnel.

En outre, le principe de *privacy by default*, tel que prévu par l'article 23.2 de la proposition de règlement, impose au responsable du traitement de mettre en œuvre des mécanismes qui portent atteinte le moins possible à la vie privée et aux données à caractère personnel des personnes concernées, en l'obligeant à choisir les options les plus protectrices des données et de la réglementation en place. Ces deux principes auront certainement des implications très concrètes pour les fournisseurs de logiciels — et notamment les navigateurs internet — qui devront en principe activer les options les plus protectrices de la vie privée par défaut, et développer des applications qui tiennent compte *avant leur conception* des exigences en matière de protection des données à caractère personnel. La Commission pourra à cet égard édicter des actes délégués pour préciser d'éventuels critères et exigences supplémentaires, ainsi que des actes d'exécution pour fixer les normes techniques relatives à la mise en œuvre des deux principes susmentionnés[49].

Enfin, l'article 10 de la proposition de règlement dispose que si les données traitées ne permettent pas au responsable du traitement d'identifier une personne physique, il n'est pas tenu d'obtenir les informations supplémentaires pour identifier la personne concernée à la seule fin de respecter une disposition du présent règlement. Cette disposition se lira idéalement en relation avec les obligations de *privacy by default* et *privacy by design*, ainsi qu'avec le principe de minimisation des données déjà évoqué[50].

D. — Les notifications des atteintes à la sécurité enfin consacrées

La proposition de règlement consacre le principe de notification des violations de données à caractère personnel, définies comme « une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation, ou la consultation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière »[51].

Les responsables du traitement doivent notifier à l'autorité de contrôle compétente, sans retard injustifié, et si possible, dans les 24 heures au plus tard après en avoir pris connaissance, toute violation de données à caractère personnel constatée par lui[52]. Une obligation similaire est imposée au sous-traitant qui doit informer le responsable du traitement en cas d'une telle violation des données. Remarquons que l'obligation de notification (« data breach notification ») avait déjà été introduite par la directive 2002/58/CE (directive *e-privacy*)[53] à l'adresse des opérateurs de réseaux publics de communications électroniques[54]. Les éléments minimums à communiquer à l'autorité de contrôle sont listés et une obligation de conserver une trace des violations de données est imposée à charge du responsable du traitement[55]. La Commission peut adopter des actes délégués pour préciser les critères et exigences applicables à l'établissement de la violation de données et concernant les circonstances particulières dans lesquelles la notification doit avoir lieu[56].

Après avoir notifié la violation de données à l'autorité de contrôle, la proposition de règlement impose au responsable du traitement de communiquer la violation aux personnes concernées lorsque celle-ci est susceptible d'avoir porté atteinte à la protection de leurs données à caractère personnel ou à leur vie privée[57]. Une telle communication aux personnes concernées n'est cependant pas nécessaire si le responsable du traitement a démontré à l'autorité de contrôle qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation[58]. Ceci encouragera certainement les responsables du traitement à mettre en œuvre des mesures techniques de sécurité permettant d'éviter de devoir communiquer aux personnes concernées toute violation de sécurité, et d'engendrer un préjudice de réputation non négligeable.

6 Un renforcement des droits des individus

Outre le renforcement de droits déjà établis par la directive 95/46 (droit à la transparence, droit d'accès et de rectification, droit d'opposition au traitement, droit à ne pas être soumis à une décision automatisée), de nouveaux droits ont été créés par la proposition de règlement. Il s'agit du droit à l'oubli, du droit à la portabilité des données et de la réglementation du profilage.

A. — Renforcement de droits existants

On remarque qu'en matière de transparence, l'information à fournir à la personne concernée est plus fouillée que dans la directive 95/46. Elle oblige, par exemple, le responsable du traitement à signaler qu'un transfert international de données est envisagé, ou encore de l'origine des données lorsqu'elles n'ont pas été collectées directement auprès de la personne concernée[59]. On constate également un renforcement du droit d'opposition, en vertu de

(46) Ainsi il se peut que la maison mère d'un groupe soit établie au Luxembourg, où se prennent les décisions relatives à l'administration de la société, mais que les décisions relatives aux traitements de données soient adoptées dans un autre État membre, où est par exemple situé le centre technique ou la filiale chargée de la gestion des données du groupe.

(47) Avis du C.E.P.D. du 7 mars 2012, p. 18.

(48) Avis 01/2012 du Groupe de l'Article 29, p. 10.

(49) Articles 23.3 et 23.4 de la proposition de règlement.

(50) Voy. avis 01/2012 du Groupe de l'article 29, p. 11.

(51) Article 4 (9) de la proposition de règlement.

(52) Article 31.1 de la proposition de règlement.

(53) Directive 2002/58/CE du Parlement européen et Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et de la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.* L 201 du 31 juillet 2002.

(54) Restera à définir comment ces deux obligations de notification, qui peuvent se recouper, vont se dérouler en pratique dès lors qu'elles sont susceptibles d'être adressées à des autorités de contrôle différentes.

(55) Article 23.3 de la proposition de règlement.

(56) Des inquiétudes sont exprimées par les autorités de protection des données quant à la charge de travail que cette obligation de notification pourrait engendrer, à la suite notamment de l'expérience américaine. Voy. à ce sujet avis du Groupe de l'Article 29 01/2012, p. 16 et C. Kuner, « The European Commission's Proposed Data Protection Regulation : A Copernican Revolution in European Data Protection Law », *Privacy and Security Law Report*, February 2012, p. 8.

(57) Article 32.1 de la proposition de règlement.

(58) En outre, de telles mesures de protection technologiques doivent rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès. Voy. article 32.2 de la proposition de règlement.

(59) L'article 11 de la directive 95/46 ne consacrait pas un tel droit à être automatiquement informé de l'origine des données. Cette information pouvait être obtenue en vertu du droit d'accès consacré par l'article 12, a), de la directive 95/46.

l'article 19 qui consacre le droit de s'opposer à tout traitement fondé sur l'article 6.1 d), e) et f) à moins que le responsable du traitement n'établisse l'existence de raisons impérieuses et légitimes justifiant le traitement[60].

B. — Le droit à l'oubli

L'une des évolutions les plus significatives concernant les droits conférés aux personnes concernées est certainement la reconnaissance d'un droit à l'oubli. L'article 17 de la proposition de règlement dispose que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel et la cessation de la diffusion de ces données[61]. Ce droit ne se limite pas à un droit à l'effacement tel qu'il existait déjà dans la directive 95/46 en son article 12 b), mais en constitue plutôt une extension, dès lors que la proposition dispose que le responsable du traitement doit prendre toutes les mesures raisonnables, y compris techniques, pour informer les tiers qui traitent également ces données que la personne concernée demande de les effacer, de ne pas les reproduire, et de ne pas les diffuser[62]. Nous sommes néanmoins perplexes quant à l'effectivité de ce droit à l'oubli[63]. En effet, il est difficile d'imposer au responsable du traitement de connaître tous les tiers qui traitent les données faisant l'objet dudit droit. C'est d'ailleurs sans doute pour cette raison que le texte n'impose qu'une obligation de moyen au responsable du traitement, qui doit prendre les « mesures raisonnables » pour informer ces tiers (on pensera par exemple spécifiquement aux moteurs de recherches qui ont dupliqué et indexé les données en question). En outre, on constate que cette information faite aux tiers est laissée sans mesure consécutive : le texte ne prévoit pas d'obligation pour le tiers de retirer les données, ni de responsabilité claire du responsable du traitement si les données ne sont pas effacées. Enfin, soulignons que la responsabilité des intermédiaires de la société de l'information est soumise à un régime d'exemption conformément aux articles 12 à 15 de la directive 2000/31/CE dite « commerce électronique »[64]. Rappelons que ce régime ne retient la responsabilité des intermédiaires de l'internet (par exemple, les hébergeurs) pour le contenu ayant transité par leurs services qu'à des conditions très strictes[65].

C. — Le droit à la portabilité des données

La proposition de règlement introduit également un droit complètement nouveau : celui pour la personne concernée d'obtenir une copie de ses données sous une forme intelligible lui permettant de les réutiliser, le tout dans un format électronique structuré[66]. Le texte prévoit en outre la possibilité pour la personne concernée de transmettre ces données « et toutes autres informations qu'elle a fournies »[67] à un autre système de traitement automatisé, sans que le responsable du traitement ne puisse s'y opposer. Le but de cette disposition est de permettre à la personne concernée, utilisatrice d'un service offert par le responsable du traitement (comme un service de réseau social par exemple), de changer de fournisseur de services sans que ses données restent prisonnières auprès du premier fournisseur. Nul doute que l'effectivité de cette obligation sera un beau défi pour la Commission, qui dispose du pouvoir d'adopter des actes d'exécution pour préciser le format électronique, ainsi que les normes techniques, les modalités et les procédures pour la transmission de données à caractère personnel conformément à ce nouveau droit.

D. — Mesures fondées sur le profilage

Ce droit n'est pas nouveau à proprement parler, mais constitue une extension de la protection des personnes concernées eu égard à l'adoption de décisions individuelles automatisées[68]. L'article 20 de la proposition de règlement adresse la problématique plus générale du profilage, qui englobe tant les mesures destinées non seulement à analyser[69] mais également à *prévoir* le comportement ou les habitudes des personnes physiques[70]. En outre, le texte de la proposition permet de n'être soumis ni à des mesures de profilage, ni à des « décisions automatisées », ce qui élargit sans aucune doute la portée de la protection offerte par le règlement par rapport à celle de la directive 95/46, dès lors que le terme « mesure » ne se limite pas à la prise de décisions, mais inclut un éventail plus large d'actions[71]. Enfin, le texte de la proposition de règlement ne fait plus référence à « un traitement de données à caractère personnel », mais bien à l'opération de profilage, indépendamment du fait que ce profilage se base sur des données à caractère personnel ou non. Sans doute l'intention de la Commission n'était pas de permettre l'application de cette disposition sans que l'on ait bien affaire à des données à caractère personnel. Cependant, on pourrait y voir là un élément intéressant concernant le champ d'application matériel de la proposition de règlement. En effet, rappelons que la question de savoir si des données non nominatives pouvaient être considérées comme des données à caractère personnel — et dans quelles hypothèses — a toute son importance concernant les traces laissées sur Internet (telles que des *cookies* ou l'adresse IP), lesquelles peuvent être utilisées par les entreprises pour dresser des profils d'utilisateurs. Dès lors, indépendamment du fait de savoir si des données traitées peuvent être considérées comme des données à caractère personnel, tout profilage, notamment dans le cadre de la publicité comportementale en ligne *(online behavioural advertising)*, pourrait être soumis aux conditions de l'article 20. Soulignons toutefois que le droit de ne pas être soumis à une mesure prise sur la base d'un traitement automatisé ne s'applique que lorsque la mesure produit des effets juridiques ou affecte de manière significative la personne concernée. Cette notion n'est malheureusement pas explicitée et il nous semble difficile de lui donner un contenu en l'absence d'indications plus claires concernant son interprétation. Malheureusement la Commission n'a pas jugé utile, cette fois, de prévoir la possibilité d'édicter des actes délégués ou d'exécution à ce sujet...

7

Le principe général de responsabilité du responsable de traitement : implications et nouvelles obligations

Au rang des principes cardinaux de la protection des données énoncés à l'article 5 de la proposition, est érigé le principe de responsabilité du responsable de traitement tenu de veiller à la conformité de chaque opération de traitement avec le règlement et d'en apporter la preuve[72]. Ce principe de *responsabilité* (communément énoncée en anglais sous le terme d'*accountability*) vise, au-delà du principe de responsabilité légale (distinguée du terme de *liability*), l'obligation pour le responsable de traitement de mettre en œuvre des mesures appropriées et efficaces pour garantir le respect des principes et obligations définies dans le règlement, responsabilité à laquelle est attaché un principe de *démonstration* du respect de ces principes et obligations[73]. Un premier exemple illustrant cette responsabilité se trouve dans la charge faite au responsable de traitement d'apporter la preuve du consentement de la personne

(60) On rappelle que l'article 14 de la directive 95/46 laissait à la personne concernée la charge de prouver qu'elle avait un intérêt légitime pour s'opposer au traitement. La proposition de règlement renverse ici la charge de la preuve.

(61) Le texte précise que ce droit peut être exercé en particulier en ce qui concerne des données que la personne concernée avait rendues disponibles lorsqu'elle était enfant, ou pour l'un des motifs énumérés à l'article 17.1. Le texte nous paraît peu clair dès lors qu'il semble ouvrir une liste non exhaustive de conditions dans lesquelles le droit à l'oubli peut s'exercer. Remarquons toutefois que la Commission peut adopter des actes délégués pour préciser les exigences et critères relatifs à l'application du paragraphe premier et des situations spécifiques impliquant le traitement de données.

(62) Article 17.2 de la proposition de règlement.

(63) Voy. avis 01/2012 du Groupe de l'Article 29, p. 13.

(64) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur, *J.O.C.E.* L 178 du 17 juillet 2000.

(65) À ce sujet, voy. E. Montero, « La responsabilité des prestataires intermédiaires sur les réseaux », in E. Montero, *Le commerce électronique européen sur les rails? - Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Cahiers du C.R.I.D, n° 19, Bruxelles, Bruylant, 2001.

(66) Article 18.1 de la proposition de règlement.

(67) Le texte semble étendre ici le champ d'application de la proposition de règlement, qui ne porte *a priori* que sur des données à caractère personnel.

(68) Article 15 de la directive 95/46.

(69) La directive 95/46 reprenait le terme « évaluer ».

(70) Ce faisant, la proposition suit une recommandation du Conseil de l'Europe en la matière : voy. recommandation CM/Rec (2010)13 du 23 novembre 2010 du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Cette recommandation définissait le profilage comme toute « technique de traitement automatisé des données qui consiste à appliquer un "profil" à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels ».

(71) Voy. Y. Poullet et L. Costa, *op. cit.*, point 8.

(72) Article 5, f), de la proposition de règlement, réitéré et spécifié à l'article 22.1.

(73) Voir les développements du Groupe de l'Article 29 dans son avis 03/2010 du 3 juillet 2010 sur le principe de responsabilité, WP 173.

concernée[74]. La proposition de règlement intègre ce principe de responsabilité en son article 22.1, mais aussi au travers de toute une série d'obligations nouvelles et spécifiques pour le responsable de traitement.

A. — Le remplacement de l'obligation de notification par la tenue d'une documentation

Outre la mise en œuvre des obligations en matière de sécurité pour le traitement de données[75] qui existent déjà dans la directive 95/46[76], il est prévu que le responsable de traitement assure la tenue d'une documentation[77] comportant les informations essentielles de tout traitement[78]. La tenue de cette documentation qui doit être mise à la disposition de l'autorité de protection des données en cas de contrôle[79] correspond largement aux informations actuellement contenues dans la notification des traitements aux autorités de protection des données[80]. Dès lors, si le règlement supprime l'obligation de *notification*, il la remplace par celle de tenir à disposition la *documentation* relative au traitement. Notons toutefois que le responsable du traitement ou le sous-traitant agissant au nom du responsable du traitement doit consulter l'autorité de contrôle dans les cas définis par l'article 34.2 de la proposition de règlement[81].

B. — L'introduction de l'obligation de réaliser des analyses d'impact

Une autre illustration du principe de responsabilité est l'obligation faite au responsable de traitement d'effectuer une analyse d'impact des traitements présentant des risques particuliers sur la protection des données avant leur mise en œuvre[82]. Une liste indicative, et non exhaustive, des traitements présentant des risques particuliers est dressée[83]. Seront ainsi soumis à une analyse d'impact les traitements de données à grande échelle aux fins de profilage des personnes en vue de l'adoption de mesures produisant des effets juridiques les affectant, certains traitements de données sensibles, l'installation de vidéosurveillance à grande échelle, le traitement de données biométriques ou génétiques de grande ampleur ou concernant des enfants et les traitements soumis à la consultation préalable de l'autorité de contrôle. Les spécifications concernant l'analyse d'impact sont en revanche succinctes et il est laissé à la Commission le soin de préciser davantage les conditions de mise en œuvre de ces analyses d'impact via l'adoption ultérieure d'actes délégués[84].

C. — La désignation d'un délégué à la protection des données

Un autre instrument illustrant le système de responsabilité mis en place par le règlement est l'obligation faite aux autorités ou organismes publics et entreprises de plus de 250 employés, agissant en tant que responsable de traitement ou sous-traitant, de désigner un délégué à la protection des données (D.P.D.)[85]. Plusieurs dispositions visant à garantir l'indépendance du D.P.D. dans l'exercice de ses fonctions sont prévues par le règlement[86]. Le D.P.D. est supposé être recruté et désigné sur la base de ses qualités professionnelles et compétences en la matière[87]. S'il est nommé pour une durée minimale de deux ans, reconductible, il ne peut être démis de ses fonctions durant son mandat[88]. Par ailleurs, si le D.P.D. assure en même temps d'autres fonctions professionnelles, celles-ci doivent être compatibles avec sa fonction de D.P.D. et ne pas entraîner de conflits d'intérêts[89]. Entre autres missions, le D.P.D. sera notamment chargé de contrôler la documentation, d'être l'interlocuteur principal de l'autorité de contrôle et de traiter les demandes d'accès, de rectification ou d'opposition des personnes concernées[90].

8

Le régime réservé à deux catégories d'acteurs : les sous-traitants et les micros, petites et moyennes entreprises

A. — Le rôle et nouvelles obligations des sous-traitants

Le projet de règlement précise les responsabilités, obligations et missions du sous-traitant[91]. Il y est notamment précisé que si le sous-traitant traite des données à caractère personnel en dehors des instructions données par le responsable de traitement, il sera considéré comme responsable de traitement à son tour[92]. Plusieurs obligations viennent s'appliquer à lui : la tenue de la documentation[93], l'obligation de coopérer avec les autorités de contrôle[94], l'obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux données à protéger qui est explicitement étendue aux sous-traitants[95], l'obligation de réaliser des analyses d'impact pour les traitements présentant des risques particuliers[96] ainsi que l'obligation de désigner un délégué à la protection des données dans les conditions citées plus haut[97]. Par ailleurs, le règlement prévoit expressément la possibilité pour les sous-traitants de procéder à des transferts internationaux moyennant des « garanties appropriées », et notamment des règles d'entreprises contraignantes[98] (voy. *infra*). Enfin, il étend le droit à réparation pour les personnes concernées des dommages causés par les sous-traitants[99] qui voient donc leur responsabilité générale engagée dans le projet de règlement au même titre que les responsables de traitement.

B. — L'assouplissement du régime pour les micros, petites et moyennes entreprises (M.P.M.E.)

L'un des objectifs annoncé de la révision du cadre de protection des données était l'assouplissement du régime pour les M.P.M.E.[100]. La proposition de règlement y procède par deux approches. La première consiste à octroyer des dérogations aux entreprises de moins de 250 salariés dont l'activité de traitement de données est accessoire à leur activité principale : dérogation à l'obligation de tenir une documentation[101], dérogation à l'obligation de désigner un représentant dans l'Union pour les responsables de traitement et sous-traitant établi à l'étranger[102] et principe d'un avertissement écrit avant toute sanction administrative pour un premier manquement non intentionnel au règlement[103]. La seconde approche consiste à laisser à la Commission européenne, dans le cadre de l'adoption d'actes délégués et d'exécution prévus dans le règlement, le soin de prévoir des mesures adaptées pour les M.P.M.E. en ce qui concerne : les exigences et critères applicables au méthodes d'obtention du consentement du parent de l'enfant[104], les mécanismes et procédures d'exercice des droits de la personne concernée[105], les conditions applicables au droit d'accès des personnes concernées[106], les critères et exigences du principe de responsabilité du responsable de traitement et du sous-traitant[107] et les conditions de mise en œuvre des analyses d'impact[108]. L'essentiel de l'assou-

(74) Article 7.1 de la proposition de règlement.
(75) Article 30 de la proposition de règlement.
(76) Article 17 de la directive 95/46.
(77) Article 22.2, a), de la proposition de règlement.
(78) Comme les noms et coordonnées du responsable, du responsable conjoint, de tout sous-traitant et du délégué à la protection des données, des finalités du traitement, une description des catégories de données et des personnes concernées, des destinataires ou catégories de destinataires des données, des délais envisagés de conservation jusqu'à l'effacement des données et le cas échéant des transferts vers les pays tiers et des garanties appropriées entourant ces transferts, selon l'article 28.2 de la proposition de règlement.
(79) Article 28.3 de la proposition de règlement.
(80) Article 18 et 19 de la directive 95/46.
(81) À savoir lorsqu'une analyse d'impact aura indiqué que le traitement présente une degré élevé de risques particuliers, ou sur la base d'une liste de traitements établie par l'autorité de contrôle qui aura estimé que ces types de traitements doivent faire l'objet d'une consultation.
(82) Articles 22.2, c), et 33.1 de la proposition de règlement.
(83) C'est ce qu'il faut déduire de l'emploi du terme « notamment » avant les traitements listés aux points a) à e), de l'article 3.2.

(84) Article 33.6 de la proposition de règlement.
(85) Articles 22.2, e), et 35.1 de la proposition de règlement.
(86) Le principe de l'indépendance du D.P.D. est énoncé à l'article 36.2 de la proposition de règlement.
(87) Article 35.5 de la proposition de règlement.
(88) Article 36.7 de la proposition de règlement.
(89) Article 35.6 de la proposition de règlement.
(90) Article 37.1 de la proposition de règlement.
(91) Article 26 de la proposition de règlement.
(92) Article 26.4 de la proposition de règlement.

(93) Article 28 de la proposition de règlement.
(94) Article 29 de la proposition de règlement.
(95) Article 30 de la proposition de règlement.
(96) Article 33 de la proposition de règlement.
(97) Article 35 de la proposition de règlement.
(98) Article 42 de la proposition de règlement.
(99) Article 77 de la proposition de règlement.
(100) Définies suivant la recommandation 2003/361/CE de la Commission européenne du 6 mai 2003.
(101) Article 28.4, b), de la proposition de règlement.
(102) Article 25.2 de la proposition de règlement.
(103) Article 79.3, b), de la proposition de règlement.
(104) Article 8.3 de la proposition de règlement.
(105) Article 12.6 de la proposition de règlement.
(106) Article 14.7 de la proposition de règlement.
(107) Article 22.4 de la proposition de règlement.
(108) Article 33.6 de la proposition de règlement.

plissement du régime pour les M.P.M.E. dépendra donc de la prise en compte de leur situation particulière à l'avenir par la Commission européenne dans les actes délégués et d'exécution à adopter.

9

Le traitement de catégories particulières de données

A. — Les données dites « sensibles »

Le traitement de catégories particulières de données, généralement désignées comme sensibles, est soumis à un principe général d'interdiction, assorti de multiples exceptions[109]. À la définition des données sensibles de la directive 95/46[110], ont été ajoutées les données génétiques[111], définies comme « les caractéristiques d'une personne physique qui sont héréditaires ou acquises à un stade précoce de son développement prénatal »[112] et les données relatives aux condamnations pénales ou autres mesures de sûreté connexes. La protection spécifique apportée à ces dernières semble d'ailleurs moins étendue que dans le régime actuel. En effet, le règlement étend l'exception de traitement de ces données sous le contrôle d'une autorité publique à d'autres responsables de traitement, qui pourraient de pas être nécessairement une autorité publique, si le traitement est nécessaire au respect d'une obligation légale ou réglementaire[113]. Le règlement introduit par ailleurs une nouvelle exception, formulée en des termes très généraux, pour le traitement des données sensibles lorsque celui-ci est nécessaire « à l'exécution d'une mission effectuée dans l'intérêt général sur le fondement du droit de l'Union ou d'un État membre » sous réserve que des garanties appropriées accompagnent ce traitement[114]. Le traitement des données relatives à la santé est permis au travers de plusieurs dispositions dispersées dans le règlement, ce qui, selon le C.E.P.D., ne rend pas leur analyse et compréhension évidente[115]. Comme dans la directive, le traitement de données sensibles nécessaire à la sauvegarde des intérêts vitaux de la personne concernée peut constituer un cas de traitement de données relatives à la santé[116]. Les cas de traitements aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de gestion de services de santé, ou ceux réalisés pour des motifs d'intérêt général dans le domaine de la santé publique ou de la protection sociale sont quant à eux prévus à l'article 81 de la proposition de règlement. Enfin, ceux réalisés à des fins de recherche historique, statistique ou scientifique sont soumis aux dispositions spécifiques de l'article 83 prévu à cet effet.

B. — Situations particulières de certains traitements de données

Le chapitre IX de la proposition de règlement entend laisser aux État membres une certaine liberté de légiférer concernant certains types de traitements, comme les traitements impliquant la liberté d'expression, les traitements de données relatives à la santé (expliqués *supra*) ou relatives aux employés, et les traitements de données à des fins de recherche historique, statistique ou scientifique. Si on peut comprendre que le texte laisse une certaine marge d'appréciation aux États membres dans ces matières, on peut s'interroger sur l'efficacité de ces mesures, et notamment sur l'absence de cohérence à laquelle elle pourrait conduire, par exemple, en matière de traitement des données des employés, dès lors que des groupes internationaux resteront soumis à la législation sociale nationale en vigueur dans chaque État membre. L'objectif d'uniformisation est donc susceptible d'être mis à mal par la marge de manœuvre laissée aux États. On pense aussi à d'autres législations touchant à la protection des données à caractère personnel dans des matières spécifiques : on admet donc que les États membres ajoutent des conditions à de tels traitements, « dans la limite du présent règlement »[117].

10

Un régime de flux transfrontières complété

L'un des grands domaines dans lesquels la refonte des règles était attendue au niveau européen et international est celui du régime des flux transfrontières de données. La proposition de règlement reprend en partie le régime existant et le complète via la reconnaissance des « Règles d'entreprises contraignantes » (*Binding Corporate Rules - B.C.R.*). En revanche, il est regrettable que la proposition de règlement ne définisse pas ce qu'il faut entendre par la notion de « transfert ». En effet, l'environnement numérique, le marché croissant du *cloud computing*, et l'ensemble de l'activité en ligne demandaient pourtant une clarification de la notion au niveau européen. La Commission européenne manque ici selon nous une occasion de se positionner clairement par rapport à la jurisprudence *Lindqvist* qui constitue la seule interprétation de la notion de transfert et qui, rappelons-le, n'a pas considéré que la publication de données sur internet par une personne physique constitue un transfert international de données[118]. La proposition semble hiérarchiser trois grandes hypothèses de transferts présentées ci-dessous.

A. — Les transferts dans la zone d'adéquation

Tout d'abord, il faut relever que le principe actuel de la prohibition des transferts vers des pays n'assurant pas un niveau adéquat de protection — sauf exceptions [119] — est levé dans la proposition de règlement. Les transferts vers des pays ou organisations internationales reconnus par décision de la Commission comme offrant un niveau adéquat de protection constitue dès lors la première hypothèse, suivie d'autres, de transferts autorisés[120]. La compétence d'adopter des décisions d'adéquation est désormais réservée à la Commission européenne. Si certains regrettent que la Commission n'apporte pas davantage de précisions concernant les critères aux fins d'évaluation du niveau de protection[121], la prise en compte de « la primauté du droit », ainsi que de la législation sectorielle pertinente concernant « la sécurité publique, la défense, la sécurité nationale et le droit pénal », « l'existence de droits effectifs et opposables », et les « engagements internationaux souscrits par le pays tiers ou l'organisation internationale »[122] nous donne des indications claires que le niveau de protection des données est évaluée dans un contexte global, où l'État de droit, mais aussi les limites d'accès du secteur policier ou du renseignement aux données transférées par le secteur privé seront prises en compte. La décision de reconnaissance d'adéquation d'un pays tiers se fondera donc sur des conditions de traitement dans ce pays qui dépassent le seul champ d'application matériel du règlement (dès lors que les traitements relatifs au droit pénal ou la sécurité nationale ne sont pas soumis à la proposition de règlement). Rappelons également que, si l'évaluation d'adéquation est générale, les décisions d'adéquations peuvent, quant à elles, être sectorielles[123].

B. — Les transferts dans le cadre de garanties appropriées inscrites dans un instrument juridiquement contraignant

Pour les cas de transferts vers des pays ou organisations n'assurant pas un niveau adéquat de protection, la proposition de règlement prévoit que le responsable de traitement ou le sous-traitant peuvent procéder aux transferts moyennant des garanties appropriées prévues dans un instrument juridiquement contraignant[124]. Outre les clauses contractuelles type adoptées par la Commission ou les transferts autorisés par une autorité de contrôle qui existent déjà dans le régime actuel de la directive 95/46[125], le règlement reconnaît expressément les règles d'entreprise contraignantes (B.C.R.) comme ga-

(109) Article 9 de la proposition de règlement.
(110) Article 8.1 de la directive 95/46.
(111) Article 9.1 de la proposition de règlement.
(112) Article 4 (10) de la proposition de règlement.
(113) Article 9.2, j), de la proposition de règlement. Voy. aussi en ce sens l'avis du C.E.P.D. du 7 mars 2012, § 135, p. 22.
(114) Article 9.2, g), de la proposition de règlement.
(115) Avis du C.E.P.D. du 7 mars 2012, pp. 48-49.
(116) Article 9.2, c), de la proposition de règlement.
(117) On peut se demander comment articuler le règlement et les principes juridiques régissant des traitements particuliers de données déjà soumis à une législation spécifique. On pense par exemple au droit à l'image, impliquant le plus souvent l'application des législations en matière de protection des données. Ces « droits spécifiques » doivent-ils s'effacer devant le règlement au nom de l'uniformisation? À ce sujet, voy. J.-F. Puyraimond, « La protection des données personnelles : nouveau fondement du droit à l'image », *J.T.*, 2008/5, pp. 364 et s.
(118) C.J.C.E., *Lindqvist*, 6 novembre 2003, aff. C-101/01.
(119) Voy. articles 25 et 26 de la directive 95/46.
(120) Article 41 de la proposition de règlement.
(121) En ce sens, voy. C. Kuner, *op. cit.*, p. 9.
(122) Article 41.2 de la proposition de règlement.
(123) Ce qui signifie que la Commission peut décider qu'un pays tiers présente un niveau de protection adéquate, mais, par exemple, uniquement dans le secteur public.
(124) Article 42.1 de la proposition de règlement.
(125) Article 26.2 de la directive 95/46.

ranties appropriées entourant les transferts internationaux. Les B.C.R. sont soumises à l'approbation d'une autorité de contrôle après consultation des autres autorités via le nouveau mécanisme de contrôle de la cohérence (voy. *infra*).

C. — **Les dérogations**

Si un flux transfrontière ne se fait pas dans la zone d'adéquation, ou en vertu de garanties appropriées résultant d'un instrument juridique contraignant (voy. *supra*), le transfert sera encore possible en vertu de dérogations. Le nouveau régime de flux transfrontières proposé dans le règlement prévoit deux catégories de dérogations. La première permet le transfert international sans que les garanties appropriées soient consignées dans un instrument juridiquement contraignant. En effet, le règlement prévoit qu'un tel transfert puisse être possible après approbation de l'autorité de contrôle[126]. La seconde catégorie de dérogations reprend principalement celles de l'article 26.1 de la directive 95/46[127]. Notons qu'on y trouve une nouvelle dérogation, à savoir la nécessité d'un transfert qui ne puisse être qualifié de fréquent ou de massif « aux fins des intérêts légitimes poursuivis par le responsable du traitement ou le sous-traitant » et offrant, après évaluation, des garanties appropriées en matière de protection des données[128]. On constate qu'un tel transfert sera donc laissé à l'appréciation du responsable du traitement ou du sous-traitant, qui sera appelé à apprécier lui-même la possibilité d'invoquer cette condition, tout en prenant en considération les éléments cités à l'article 44.3.

11

La mise en œuvre du règlement

A. — **Un renforcement et une harmonisation du rôle des autorités de contrôle**

Les États membres devront choisir une ou plusieurs autorités de contrôle pour veiller à l'application des dispositions de la proposition de règlement[129]. Les articles 47 à 48 confirment que ces autorités devront être indépendantes, et précisent les contours de cette notion d'un point de vue structurel, mais aussi fonctionnel[130].

Le choix d'un règlement comme instrument législatif entraîne que, si la question du droit applicable ne se pose plus, il subsiste néanmoins la question de savoir quelle(s) autorité(s) de contrôle sera(ont) compétente(s), lorsque le responsable du traitement est établi dans plusieurs États membres. Pour régler cette question, l'article 51.2 dispose que l'autorité compétente sera celle de l'État membre où se situe l'établissement principal du responsable du traitement ou du sous-traitant, le tout sans préjudice du mécanisme de coopération et de cohérence mis en place par la proposition de règlement[131].

Devant le constat selon lequel les critères de compétence retenus n'étaient pas des plus clairs, ni des plus satisfaisants, les autorités de contrôle prônent l'introduction du critère d'« influence dominante »[132] pour expliciter la notion d'« établissement principal », qui serait déterminé par plusieurs éléments[133]. Elles appellent également à l'introduction du concept « d'autorité chef de file » (*lead authority*), qui serait l'autorité de référence pour les responsables du traitement et les sous-traitants[134]. Notons que la question de savoir qui sera l'autorité compétente lorsque le responsable du traitement n'est pas établi sur le territoire de l'Union n'est pas abordée par la proposition de règlement, ce qui constitue une lacune qui devra sans doute être comblée.

Les fonctions des autorités de contrôle sont harmonisées et leurs pouvoirs explicitement mentionnés[135]. On citera le pouvoir d'interdire définitivement ou temporairement un traitement, de suspendre un transfert international de données, ou encore d'imposer des sanctions. Il est certain que cette liste aboutira à un renforcement des pouvoirs des autorités de contrôle dans plusieurs État membres, où elles ne disposent pas encore de telles prérogatives.

B. — **Mécanismes de coopération et de cohérence**

La proposition de règlement renforce la coopération entre les autorités de contrôle, en décrivant les obligations d'assistance mutuelle[136] et la possibilité d'opérations conjointes des autorités de contrôle[137].

Elle institutionnalise un « Comité européen de protection des données » (ComitéEPD) qui succède au Groupe de l'Article 29, dont le secrétariat serait assuré par l'actuel C.E.P.D.[138] et dont les missions et le mode de fonctionnement sont fixés par les articles 64 à 72. À côté du ComitéEPD, la Commission devient quant à elle un acteur majeur de la protection des données, puisqu'elle reçoit le pouvoir d'adopter des actes délégués et d'exécution, mais également d'assurer l'« application correcte et cohérente » du règlement[139].

Le mécanisme de cohérence qu'elle instaure est ambitieux : une autorité de contrôle doit communiquer au ComitéEPD tout projet de « mesure » dans plusieurs hypothèses, et notamment si ce projet de mesure se rapporte aux traitements liés à l'offre de biens ou de services à des personnes concernées dans plusieurs État membres ou à l'observation de leur comportement, ou est susceptible d'affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union[140]. Il va sans dire que cette obligation de communication sera plus que souvent activée, surtout lorsque la décision concernera le traitement de données sur Internet ou un traitement effectué par une entreprise internationale. Une telle procédure est donc susceptible de se révéler très vite lourde pour les autorités de protection de données[141].

Le ComitéEPD peut décider d'émettre une opinion, dont l'autorité de contrôle nationale devra tenir compte, et communiquer en retour à la Commission et au C.E.P.D. si elle adopte la mesure ou non[142].

La Commission, quant à elle, s'octroie un grand pouvoir d'influence, dès lors qu'elle peut exiger que certaines décisions soient examinées dans le cadre du mécanisme de contrôle et de cohérence[143]. Elle peut en outre communiquer une opinion, tout comme le ComitéEPD, dont l'autorité de contrôle doit tenir « le plus grand compte »[144]. La Commission peut enfin enjoindre à l'autorité de contrôle de suspendre sa décision pour une durée de douze mois au maximum[145]. Cette intervention de la Commission dans le mécanisme de cohérence est vivement critiquée, dès lors que l'indépendance des autorités de contrôle est susceptible d'en souffrir[146].

C. — **Responsabilité et sanctions**

La proposition de règlement confirme que tout individu a le droit d'adresser une réclamation auprès d'une autorité de contrôle. Soulignons qu'est également reconnu aux organisations de défense des droits des personnes concernées le droit d'introduire une réclamation au nom de plusieurs personnes concernées ou en leur nom, ce qui constitue une évolution intéressante[147].

Un recours juridictionnel est également garanti contre les autorités de contrôle[148] ainsi que contre un responsable du traitement ou un sous-traitant[149]. Une telle action juridictionnelle peut être intentée devant les tribunaux de l'État membre où est situé le responsable du traitement ou le sous-traitant, mais aussi devant les tribunaux de l'État membre dans lequel la personne concernée a sa résidence habituelle,

(126) Article 42.2 de la proposition de règlement.
(127) Article 4.1, a) à f), de la proposition de règlement.
(128) Article 44.1, h), de la proposition de règlement.
(129) Article 46 de la proposition de règlement.
(130) Rappelons que la C.J.U.E. a eu l'occasion d'interpréter strictement le principe d'indépendance des autorités de contrôle dans son arrêt *Commission c. Allemagne* du 9 mars 2010, aff. C-518/07.

(131) Voy. *infra*.
(132) Ce concept est d'ailleurs déjà introduit dans le considérant 28 au sujet des groupes d'entreprises. Il conviendra de ne pas créer de confusion entre les notions utilisées.
(133) Sur la notion d'« influence dominante », voy. avis 01/2012 du Groupe de l'Article 29, pp. 10 et 18.
(134) Avis 01/2012 du Groupe de l'Article 29, p. 19; Information Commissioner's Office : *Initial analysis of the European Commission's proposal for a revised data protection legislative framework*, *op. cit.*, p. 22.
(135) Article 53 de la proposition de règlement.
(136) Article 55 de la proposition de règlement.
(137) Article 56 de la proposition de règlement.
(138) Contrôleur européen de protection des données.
(139) Voir notamment l'article 58.4 de la proposition de règlement.

(140) Article 59.2 de la proposition de règlement.
(141) Information Commissioner's Office : *Initial analysis of the European Commission's proposal for a revised data protection legislative framework*, *op. cit.*, p. 24.
(142) Article 58.4 à 58.8 de la proposition de règlement.
(143) Article 58.4 de la proposition de règlement.
(144) Article 59 de la proposition de règlement.
(145) Article 60 de la proposition de règlement.
(146) Information Commissioner's Office : *Initial analysis of the European Commission's proposal for a revised data protection legislative framework*, *op. cit.*, p. 25, avis 01/2012 du Groupe de l'Article 29, p. 20; avis du C.E.P.D. du 7 mars 2012, pp. 40-42.
(147) Article 73 de la proposition de règlement.
(148) Article 74 de la proposition de règlement.
(149) Article 75 de la proposition de règlement.

sauf si le responsable du traitement est une autorité publique agissant dans l'exercice de ses prérogatives de puissance publique[150].

Outre un droit à obtenir réparation des dommages causés par la violation du règlement[151], le texte prévoit que les États membres devront définir les sanctions pénales adéquates dans leur législation interne[152].

La grande nouveauté réside sans aucun doute dans le pouvoir conféré aux autorités de contrôle d'infliger des sanctions administratives en cas de violation des dispositions du règlement[153]. Le montant des sanctions est établi et détaillé par la proposition, en paliers, en fonction de la gravité de l'infraction constatée, mais également en fonction du chiffre d'affaires annuel de l'entreprise concernée. On ne peut que se réjouir de ces dispositions, qui vont enfin donner à certaines autorités de contrôle des pouvoirs de sanction dont elles ne disposaient pas auparavant.

D. — Les pouvoirs de mise en œuvre et d'exécution de la Commission

Notons que la Commission peut adopter des actes délégués ou des actes d'exécution pour préciser ou exécuter plusieurs dispositions du règlement. Cette prérogative a été vivement critiquée[154]. En effet, le nombre important de décisions que la Commission peut adopter concernant l'interprétation ou l'exécution du règlement rend sa mise en œuvre très dépendante de l'intervention de la Commission, et de nombreuses dispositions dépendent immédiatement de l'adoption de tels actes[155]. Ces derniers sont parfois essentiels pour l'application ou la compréhension de certaines dispositions du règlement. C'est pour cette raison que le Groupe de l'Article 29 souhaitait que la Commission présente un agenda pour l'adoption de tels actes[156].

C

Conclusion

La proposition de règlement de la Commission européenne n'a pas suscité un accueil unanime. Il faut souligner qu'en dépit d'une opinion globalement favorable, les réserves exprimées tant par le Groupe de l'Article 29 que le C.E.P.D. présagent d'ores et déjà d'un chemin législatif long et certainement difficile. Tandis que les autorités de protection des données belges et roumaines ont indiqué ne pas soutenir le choix d'un règlement comme instrument législatif approprié, l'autorité estonienne a émis une opinion dissidente à celle du Groupe de l'Article 29[157]. Des inquiétudes quant à l'effectivité du niveau de protection des données ambitionnée ont aussi été soulevées, notamment en ce qui concerne le critère de l'établissement principal du responsable de traitement[158]. Enfin, le mécanisme de coopération et de cohérence proposé au niveau européen et les pouvoirs importants d'implémentation octroyée à la Commission européenne ne manquent pas de crisper certaines autorités nationales et législateurs nationaux qui y voient la confiscation de leurs compétences[159]. Nul doute que les débats entourant cette proposition vont se poursuivre, et ceci, au-delà des premiers commentaires livrés dans la présente contribution.

(150) Article 75.2 de la proposition de règlement.
(151) Article 77 de la proposition de règlement.
(152) Article 78 de la proposition de règlement.
(153) Article 79 de la proposition de règlement.
(154) Avis 01/2012 du Groupe de l'Article 29, p. 7; avis du C.E.P.D. du 7 mars 2012, p. 12
(155) En outre, la conformité de ces pouvoirs avec le TFUE a également été mise en cause par le C.E.P.D., dans son avis du 7 mars 2012, p. 12.
(156) Avis 01/2012 du Groupe de l'article 29, p. 7.
(157) *Ibidem*, p. 32, voy. aussi avis de subsidiarité de la Chambre des représentants de Belgique du 6 avril 2012.
(158) Voy. UK Information Commmisoner's Office : *Initial analysis of the European Commission's proposal for a revised data protection legislative framework*, *ibidem*.
(159) Voy. notamment résolution européenne de l'Assemblée nationale française sur la proposition de règlement du 23 mars 2012, points 13-14.